HEINONLINE

Citation: 1 William H. Manz Federal Copyright Law The Histories of the Major Enactments of the 105th I 1999

Content downloaded/printed from HeinOnline (http://heinonline.org) Mon Apr 8 19:18:52 2013

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

COPYRIGHT PIRACY, AND H.R. 2265, THE NO ELECTRONIC THEFT (NET) ACT

BEST COPY AVAILABLE

HEARING

BEFORE THE

SUBCOMMITTEE ON
COURTS AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

FIRST SESSION

COPYRIGHT PIRACY, AND H.R. 2265, THE NO ELECTRONIC THEFT (NET) ACT

SEPTEMBER 11, 1997

Serial No. 47



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
48-724 CC WASHINGTON : 1997

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [I] 1999

COMMITTEE ON THE JUDICIARY

HENRY J. HYDE, Illinois, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL McCOLLUM, Florida
GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVEN SCHIFF, New Mexico
ELTON GALLEGLY, California
CHARLES T. CANADY, Florida
BOB INGLIS, South Carolina
BOB GOODLATTE, Virginia
STEPHEN E. BUYER, Indiana
SONNY BONO, California
ED BRYANT, Tennessee
STEVE CHABOT, Ohio
BOB BARR, Georgia
WILLIAM L. JENKINS, Tennessee
ASA HUTCHINSON, Arkansas
EDWARD A. PEASE, Indiana
CHRISTOPHER B. CANNON, Utah

JOHN CONYERS, JR., Michigan
BARNEY FRANK, Massachusetts
CHARLES E. SCHUMER, New York
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
STEVEN R. ROTHMAN, New Jersey

THOMAS E. MOONEY, *Chief of Staff-General Counsel*
JULIAN EPSTEIN, *Minority Staff Director*

SUBCOMMITTEE ON COURTS AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
SONNY BONO, California
EDWARD A. PEASE, Indiana
CHRISTOPHER B. CANNON, Utah
BILL McCOLLUM, Florida
CHARLES T. CANADY, Florida

BARNEY FRANK, Massachusetts
JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts

MITCH GLAZIER, *Chief Counsel*
BLAINE MERRITT, *Counsel*
VINCE GARLOCK, *Counsel*
DEBBIE K. LAMAN, *Counsel*
ROBERT RABEN, *Minority Counsel*

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [II] 1999

CONTENTS

HEARING DATE

Page

September 11, 1997 1

OPENING STATEMENT

Coble, Hon. Howard, a Representative in Congress from the State of North Carolina, and chairman, Subcommittee on Courts and Intellectual Property 1

WITNESSES

Attaway, Fritz E., Senior Vice President, Government Relations and Washington General Counsel, Motion Picture Association of America 148
Di Gregory, Kevin, Deputy Attorney General, U.S. Department of Justice 14
Goodlette, Bob, a Congressman from the State of Virginia 5
Nimmer, David, Irell and Manella, LLP 152
Peters, Marybeth, Register of Copyrights, Copyright Office of the United States 8
Sellers, Sandra A., Software Publishers Association 38
Sherman, Cary, Senior Executive Vice President and General Counsel of the Recording Industry Association of America 145
Smith, Brad, Associate General Counsel, International Law and Corporate Affairs, Microsoft Corporation 34
Wrenn, Greg, Senior Corporate Counsel, Adobe Software 32

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Attaway, Fritz E., Senior Vice President, Government Relations and Washington General Counsel, Motion Picture Association of America: Prepared statement 149
Di Gregory, Kevin, Deputy Attorney General, U.S. Department of Justice: Prepared statement 17
Goodlette, Bob, a Congressman from the State of Virginia: Prepared statement 7
Nimmer, David, Irell and Manella, LLP: Prepared statement 154
Peters, Marybeth, Register of Copyrights, Copyright Office of the United States: Prepared statement 10
Sellers, Sandra A., Software Publishers Association: Prepared statement 40
Smith, Brad, Associate General Counsel, International Law and Corporate Affairs, Microsoft Corporation: Prepared statement 35

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [III] 1999

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [IV] 1999

COPYRIGHT PIRACY, AND H.R. 2265, THE NO ELECTRONIC THEFT (NET) ACT

THURSDAY, SEPTEMBER 11, 1997

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

The Subcommittee met, pursuant to notice, at 10:03 a.m. in Room 2237, Rayburn House Office Building, Hon. Howard Coble (Chairman of the Subcommittee) presiding.

Present: Representatives Howard Coble, Bob Goodlatte, Sunny Bono, Edward A. Pease, Christopher B. Cannon, Barney Frank, Howard L. Berman, Zoe Lofgren, William D. Delahunt.

Also present: Mitch Glazer, chief counsel; Blaine Merritt, counsel; Vince Garlock, counsel; Debbie Laman, counsel; Robert Baben, minority counsel, and Eunice Goldring, staff assistant.

OPENING STATEMENT OF CHAIRMAN COBLE

Mr. COBLE. Good morning, ladies and gentlemen. As you all know, we try to be timely here. You all have gone through the effort to be here at 10:00, so I believe in starting it when you are ready to go.

Unlikely enough, I just came from the Crime Subcommittee where a hearing is being conducted on the subject of cellular telephone fraud. Today we are going to be discussing electronic copyright policy.

I guess the lesson we would learn from this, folks, is that there are a good number of Americans who enjoy stealing. Thievery, larceny, fraud, piracy, call it what you will. It is in their blood, and even in some instances, even when they do not realize remuneration or gain from it. Just the thrill of stealing.

You hear some people ask, well, in the Congress, how long are they going to be up here, and many of them will respond, "Well, I am too old to work and too nervous to steal," so "I am going to stay here for a while is the answer."

Many people are not too nervous to steal. In fact, they enjoy it. They enjoy the thrill of it.

So that is going to be the purport of our hearing today. We will hear testimony about electronic piracy of copyrighted works, a growing problem that startles individual and corporate creativity, thereby compromising the economic health of our country.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 1 1999

In addition to exploring the extent to which copyright infringement flourishes over the Internet, we hope to evaluate ongoing Executive Branch and private industry responses to electronic piracy.

Most importantly, and if possible, we need to identify other ways the Subcommittee can assist in those efforts.

Along these lines, we will also examine a legislative proposal developed by our Subcommittee member, Bob Goodlatte of Virginia. His Bill, H.R. 2265, the No Electronic Theft or Net Act, represents an important legislative response to those persons who cavalierly appropriate copyrighted works and share them with other Internet thieves.

Industry groups estimate that counterfeiting and piracy of intellectual property, especially computer software, compact discs and movies, cost the effective copyright holders more than $11 billion last year. Some claim the actual figure is closer to $20 billion.

Regrettably, the problem has great potential to worsen. The advent of digital video discs and the development of new audio compression techniques, to cite two prominent examples, will only create additional incentive for copyright thieves to steal protected works.

While our hearing is not restricted to the merits of 2265, I want to emphasize that this is not a forum to air complaints about other bills addressing extraneous issues that will be evaluated by the Subcommittee on other days.

More specifically, I want all of our witnesses to understand that we are not here this morning to discuss the on-line service copyright liability of the WIPO Treaty Bill. Now will be for another day, and we will indeed have hearings on that.

I want to—that said, I want to direct the balance of my comments to Mr. Goodlatte's bill, which will deter copyright piracy by further criminalizing the act in a firm, fair manner.

The NET Act constitutes a legislative response to the so-called *LaMacchia* case, a 1994 decision, altered by a Massachusetts Federal Court. The style of that case is *LaMacchia.* OK. I was close.

In *LaMacchia,* the defendant encouraged lawful purchases of copyrighted software and computer gauged to upload these works by a special password to an electronic bulletin board on the Internet.

The defendant then transferred the works to another electronic address and encouraged others with access to a second password to download the materials for personal use without authorization by or compensation to the copyright owners.

While critical of the defendant's behavior, the court precluded his prosecution under a Federal wiretap statute stating that this area of the law was never intended to cover copyright infringement.

The court's dictated that Congress has treaded cautiously and deliberately in amending the copyright Act, especially when devising criminal penalties for infringement.

It is self-evident that this transgression, that is, the unauthorized access to a company's products, has even greater potential to ruin small start-up companies.

Let us not forget that small businesses still comprise that sector of our national economy which provides the most employment opportunities for American citizens.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 2 1999

Thousands of independent hackers, motivated like *LaMacchia,* will cause harm to our nation's workers and the small businesses which employ them.

LaMacchia's behavior was not trivial. It deserves to be criminalized.

Accordingly, the NET Act would proscribe the willful act of copyright infringement either for commercial advantage or for profit for natural gain, all by reproducing or distributing one or more copies of copyright works which have a retail value of $5,000 or more.

In direct response to *LaMacchia,* the legislation specifically encompasses acts of reproduction or distribution that cover via transmission or computer theft.

In addition, financial gain is defined as receiving anything of value, including the receipt of other copyrighted works.

This change would enable the Department of Justice to pursue a *LaMacchia* like defendant who steals copyrighted works, but gives them away in lieu of selling them to others.

The legislation includes stiff penalties and prison terms for infringers.

The bottom line is that the public must come to understand that intellectual property rights, while abstract and arcane in many instances, probably in most instances, are no less deserving of protection than personal or real property rights.

The intellectual property community will continue its work in educating the public about these concerns, but we, in the Congress, must do our job, as well, by ensuring that piracy of copyrighted works will be treated with the appropriate level of fair, but serious, disapproval.

Again, I commend Representative Goodlatte for his leadership in this regard and look forward to working with him, as well as the other members of the Subcommittee, and our witnesses today as we consider the NET Act and other tools to combat electronic piracy.

I am now pleased to recognize the ranking member of the Subcommittee, the gentleman from Massachusetts, Mr. Frank.

Mr. FRANK. Thank you, Mr. Chairman. I will talk about as an example of the bipartisan nature of this, that you will note that the Chairman has selected me as his enunciation tutor, which is not a choice everybody would make, Mr. Chairman. I do have to say up there in Massachusetts, we would disclaim responsibility ultimately for the name, "LaMacchia." It does have other ethnic origins. Adams, we would be the experts on. *LaMacchia* probably goes elsewhere, but it is *LaMacchia,* as I understand it.

I am not really going to try to instruct you in the pronunciation of the acronym, WIPO.

What the Chairman said is my point. We are about to enter a phase in the deliberations of this Subcommittee and ultimately, I hope in the full House of the Congress, of a very important, intellectual challenging, wholly non-partisan set of issues, and a wholly non-ideological set of issues. And I will look forward to a series of hearings where we learn from the people who are here, and I congratulate the Chairman for the tone he set. We have a very important set of issues to deal with here.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 3 1999

In general, the issue that we are dealing with today will be a very important one. How do we protect the very important values of copyright?

How do we protect creative people because it is morally right to do that, and to make sure that we encourage continued creativity, from which we all benefit, while at the same time making sure that the public has the full benefit of the new technology and information that is available.

In particular, I am especially concerned that we not act in ways that would require additional censorship in any way, shape or form, by the providers, and balancing that with the importance of protecting creativity which at times is difficult.

I do not think it is difficult today. I think the Bill that our colleague from Virginia, who has been a leader in this field, brings forward is a very simple one, and I just want to address what seems to me a disturbing tendency in some parts of the country to think that talent justifies abuse of others' rights.

The fact that it may require some special skills to deprive other people of their intellectual property rights does not in any way, shape or form mitigate the viciousness of the offense.

And the fact that people are doing this as a hobby, the fact that they are doing it just to show off to other people that they are doing it and may not be directly or even directly benefitting financially is irrelevant. I say, "indirectly," because I would say that in many cases where this sort of abuse goes forward, as in the case that we're talking about, even where there is no direct financial benefit, the people who are showing off their ability to manipulate the technology, to abuse the rights of others, probably figure that they will be able to make that payoff at some point. But whether they do or do not is irrelevant.

There simply is no right, just because people are skillful, to take other people's property. Hacker should not be a way of converting the meaning of the word, "thief," into something that is socially acceptable, and that is what we do here today. We make sure that thieves of other people's intellectual property do not get away with it.

And to be very clear, too, for many of us, I will say this, and I wish I could write more formidably. I wish writing came easily to me.

But what if I have written something and witnessed, having that stolen from me, having that abuse would bother me more than losing a few hundred bucks. And so the notion that somehow this is not real theft, when we are talking about the appropriation of other people's intellectual property, is simply wrong.

This is a very important first step. As I said, it is an easier one. We will get into more difficult issues as we do the balancing.

But I appreciate the Chairman's bringing this forward and the last point I want to make is this:

We will be told by some people, "Well, we shouldn't legislate. Let this all be worked out.

I want to make my position on this very clear.

I have never been particularly impressed with guilt socialism. The notion that you let people in particular employment groups work these things out among themselves seems to me a terrible

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 4 1999

idea, and I think we have as the responsibility to make good public policy here.

Some people who come before us and tell us, "Well, yeah. You are right, but" what is that move—what is that worker will move me at the beginning.

I am prepared to listen to people's comments about this, but I think that it is important that we move forward, and I thank you, Mr. Chairman, for initiating. I think it can be a very fruitful period.

Mr. COBLE. I thank the gentleman, and what I am about to say, folks, has nothing to do with the hearing at hand.

What the gentleman from Massachusetts regarded by the pronunciation of a word, I recall—I am going to revert ten years now. Mr. Frank was chairing, I think the administrative law, and I was a member of that Committee. And at the conclusion of the hearing, as I was departing the room, I heard one of the—it was either a witness or a reporter. He said to a bystander: "The trouble with this hearing was that Coble talks too slow and Frank talks too fast." So, that probably has not changed too much.

Folks, as you all know, we normally restrict opening statements to the Chairman and the ranking member, but I think I would be remiss if I did not recognize the gentleman from the Roanoke Valley who authored this very important piece of information. The gentleman from Roanoke Valley, Mr. Goodlatte.

STATEMENT OF BOB GOODLETTE, A CONGRESSMAN FROM THE STATE OF VIRGINIA

Mr. GOODLATTE. Well, thank you, Mr. Chairman. And first I would like to say that I would be willing to pay more than a few hundred bucks to get something that Barney put down in writing, because I could then study it carefully rather than try to follow it when he speaks.

Mr. Chairman, I would like to thank you for holding today's important hearing, not only on legislation I have introduced, H.R. 2265, the Electronic Theft Act, but also on the larger issue of electronic copyright piracy.

Additionally, I would like to thank you, Ranking Member Frank, and our friend and colleague from Utah, Mr. Cannon, for co-sponsoring this legislation.

The NET Act closes a loophole in our nation's criminal copyright law and gives law enforcement the tools it needs to bring to justice individuals who steal the products of America's authors, musicians, software producers and others.

Additionally, the Bill will promote the dissemination of creative works online and help consumers realize the promise and potential of the Internet.

The Internet is a tremendous opportunity. Its true potential, however, lies in the future when students and teachers can access a wealth of high-quality information through the click of a computer mouse, and businesses can bring the benefits of electronic commerce to consumers.

Before this can happen, the creators must feel secure that when they use this new medium, they are protected by laws that are as effective in cyberspace as they are on Main Street.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 5 1999

The NET Act clarifies that when individuals sell pirated copies of software, recordings, movies or other creative works, or intentionally take part in works and distribute them to others, even if they do not intend to profit personally, such individuals are stealing.

The legislation affirms the belief that intellectual property is no less valuable than real property.

The Internet allows a single computer program or other copyrighted work to be illegally distributed to millions of users virtually without cost if an individual intentionally makes it available on a server and points others to the location. It is unacceptable that this activity can be carried out by individuals without fear of criminal prosecution.

Pirating works online is the same as shoplifting a videotape, book or computer program from a department store. Through a loophole in the law, however, copyright infringers who intentionally pirate works, as long as they do not do so for profit, are outside the reach of our nation's law enforcement officials.

This bizarre situation has developed because the authors of our copyright laws did not and could not have anticipated the nature of the Internet which has made the theft of all sorts of copyrighted works virtually cost-free and anonymous.

Imagine the same situation occurring with tangible goods that could not be transmitted over the Internet, such as an individual copying popular movies onto hundreds of blank tapes and passing them out on every street corner, or copying personal software onto blank disks and freely distributing them throughout the world.

Few would disagree that such activities amount to theft and should be prosecuted. We should be no less vigilant when such activities occur on the Internet.

The NET Act of 1997 makes it a felony to willfully infringe a copyright by reproducing or distributing ten or more copyrighted works with a value of at least $5,000 within a 180-day period, regardless of whether the infringing individual realized any commercial advantage or private financial gain.

It also clarifies an existing portion of the law that makes it a crime to willfully infringe a copyright for profit or personal financial gain. It does so by specifying that receiving other copyrighted works in exchange for pirated copies, bartering, is as unlawful as simply selling pirated works for cash.

Initially, the NET Act calls for victim impact statements during sentencing and directs the sentencing commission to determine a sentence strong enough to deter these crimes.

The United States is the world leader in intellectual property. We export billions of dollars' worth of creative works every year in the form of software, movies, recordings and other products.

By closing this loophole in our copyright law, the NET Act sends the strong message that we value the creations of our citizens and will not tolerate the theft of our intellectual property.

Mr. Chairman, thank you for holding this hearing today on what I feel is a very important issue for Congress to address.

I look forward to hearing from each of the witnesses who will be testifying before us today.

[The Statement of Mr. Goodlatte follows.]

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 6 1999

PREPARED STATEMENT OF BOB GOODLATTE, A CONGRESSMAN FROM THE STATE OF VIRGINIA

The House Judiciary Subcommittee on Courts and Intellectual Property held a hearing today on legislation introduced by Congressman Bob Goodlatte, (R–VA) called the No Electronic Theft (NET) Act of 1997, H.R. 2265.

The following is Goodlatte's official statement:

Mr. Chairman, I would like to thank you for holding today's important hearing not only on legislation I have introduced—H.R. 2265, the No Electronic Theft (NET) Act—but also on the larger issue of electronic copyright piracy. Additionally, I would like to thank you, Ranking Member Frank, and our friend and colleague from Utah, Mr. Cannon, for cosponsoring this legislation.

The NET Act closes a loophole in our nation's criminal copyright law, and gives law enforcement the tools it needs to bring to justice individuals who steal the products of America's authors, musicians, software producers, and others. Additionally, the bill will promote the dissemination of creative works online and help consumers realize the promise and potential of the Internet.

The Internet is a tremendous opportunity. Its true potential, however, lies in the future, when students and teachers can access a wealth of high quality information through the click of a computer mouse, and businesses can bring the benefits of electronic commerce to consumers. Before this can happen, creators must feel secure that when they use this new medium, they are protected by laws that are as effective in cyberspace as they are on main street.

The NET Act clarifies that when individuals sell pirated copies of software, recordings, movies, or other creative works, or intentionally take pirated works and distribute them to others even if they do not intend to profit personally, such individuals are stealing. The legislation affirms the belief that intellectual property is no less valuable than real property.

The Internet allows a single computer program or other copyrighted work to be illegally distributed to millions of users, virtually without cost, if an individual intentionally makes it available on a server and points others to the location. It is unacceptable that this activity can be carried out by individuals without fear of criminal prosecution.

Pirating works online is the same as shoplifting a video tape, book, or computer program from a department store. Through a loophole in the law, however, copyright infringers who intentionally pirate works, as long as they do not do so for profit, are outside the reach of our nation's law enforcement officials. This bizarre situation has developed because the authors of our copyright laws did not and could not have anticipated the nature of the Internet, which has made the theft of all sorts of copyrighted works virtually cost-free and anonymous.

Imagine the same situation occurring with tangible goods that could not be transmitted over the Internet, such as an individual copying popular movies onto hundreds of blank tapes and passing them out on every street corner, or copying personal software onto blank disks and freely distributing them throughout the world. Few would disagree that such activities amount to theft and should be prosecuted. We should be no less vigilant when such activities occur on the Internet.

The NET Act of 1997 makes it a felony to willfully infringe a copyright by reproducing or distributing ten or more copyrighted works, with a value of at least $5,000, within a 180-day period, regardless of whether the infringing individual realized any commercial advantage or private financial gain. It also clarifies an existing portion of the law that makes it a crime to willfully infringe a copyright for profit or personal financial gain. It does so by specifying that receiving other copyrighted works in exchange for pirated copies—bartering—is as unlawful as simply selling pirated works for cash. Additionally, the NET Act calls for victim impact statements during sentencing and directs the sentencing commission to determine a sentence strong enough to deter these crimes.

The United States is the world leader in intellectual property. We export billions of dollars worth of creative works every year in the form of software, movies, recordings, and other products. By closing this loophole in our copyright law, the NET Act sends the strong message that we value the creations of our citizens and will not tolerate the theft of our intellectual property.

Mr. Chairman, thank you for holding this hearing on what I feel is a very important issue for Congress to address. I look forward to hearing from each of the witnesses who will be testifying before us today.

Mr. COBLE. I thank the gentleman.

The other members have opening statements they wish to make?

(No response.)

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 7 1999

Very well. The first witness this morning is—one of them is unknown to none in the room, the Honorable Marybeth Peters, who is the registrants of copyrights for the United States.

Ms. Peters has also served as Acting General Counsel to the Copyright Office as Chief of both the Examining and Information and Reference Divisions.

She has served as consultant on copyright law in the World Intellectual Property Organization, and authored the general guide for Copyright Act of 1976.

Our next witness is Kevin Di Gregory, a Deputy Assistant Attorney General in the Criminal Division of the United States Department of Justice. He has spent his entire legal career as a trial prosecutor, beginning in 1979 in the District Attorney's office in his native Pittsburgh, Pennsylvania. Prior to coming to the Justice Department, he served as Janet Reno's Chief Assistant for Major Crimes in Miami, Florida. His current responsibilities serving as a department representative on the Executive Working Group for Federal, State and Local Prosecutors.

This group was established in 1980 to promote cooperation among all law enforcement agencies.

Mr. Di Gregory supervises two of the Criminal Division's litigating sections, the Computer Crime and Intellectual Property Section, and the Child Exploitation and Obscenity Section.

In addition, he has worked closely with the Terrorism and Violent Crime Section in the development and implementation of the Attorney General's National Anti-Violent Crime Initiative.

Because of his expertise in capital litigation, Mr. Di Gregory, along with three other senior Justice Department lawyers, served as a member of the Attorney General's Capital Case Review Committee. This Committee reviews every indictment charging a capital offense brought by the United States and advises the Attorney General on whether the death penalty should be sought.

We have written statements from both the witnesses on this panel, which I ask unanimous consent to submit into the record in their entirety.

I ask both witnesses if you will, not only you, Ms. Peters and Mr. Di Gregory, but all subsequent witnesses, if you will all try to confine your statements to the five minute rule.

We have a red light that will illuminate ominously in your face at the completion of five minutes.

We will not cane haul anyone who violates it, but if you will extend that courtesy because we have many balls in the air today, and if we can do that, we can move along at a more rapid pace.

Ms. Peters.

STATEMENT OF MARYBETH PETERS, REGISTER OF COPYRIGHTS, COPYRIGHT OFFICE OF THE UNITED STATES

Ms. PETERS. Thank you. Mr. Chairman, members of the Subcommittee, I appreciate the opportunity to testify on the No Electronic Theft Act of 1997.

The Copyright Office supports the purpose and approach of the Bill which would amend the law regarding criminal copyright infringement, to cover willful piracy that may cause serious commercial harm, despite the infringer's lack of a profit motive.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 8 1999

We agree with the sponsors of the Bill that a significant loophole exists. Deliberate and destructive piracy escapes criminal penalties when done for motives other than financial gain.

In order to preserve legitimate markets for copyrighted works, it is critical, especially in the era of digital transmission, to close this loophole quickly.

While we have a few concerns about some of the specific language of the Bill, we are confident that these concerns can be addressed.

Today, copyright owners lose an enormous sums of money to piracy. Digital technology has the potential to greatly exacerbate the problem. It allows users to make multiple copies in an instant without requiring a major investment in physical manufacturing and distribution facilities.

It has become easy for those without a commercial stake or profit motive, for example, a disgruntled former employee, a dissatisfied customer, an Internet user opposed to the fundamental concepts of copyright law, to do tremendous damage to the market for copyrighted work.

In contrast to the traditional analog world, substantial commercial harm may easily be caused by the act of a single person without any commercial aspect to the piracy itself.

Moreover, for such infringers, civil remedies are less likely to serve as an effective deterrent. Therefore, criminal sanctions are needed to deter these individuals from causing serious harm to the value of copyright works.

Currently, infringement is a crime only when it is done willfully for purposes of commercial advantage or private financial gain. As Mr. Coble noted, the *LaMacchia* case drew attention to the current law's shortcomings.

Because *LaMacchia* lacked a commercial motive, the government charged him with wire fraud rather than criminal copyright infringement. The court, in dismissing the indictment, noted that copyright infringement can be prosecuted only under the copyright law.

LaMacchia demonstrates that in a digital environment, the lack of criminal penalties for willful, non-commercial infringement is a loophole.

The court, itself, decried this loophole or concluded that LaMacchia's conduct could be a crime only if Congress acted.

H.R. 2265 responds to the court's call for a legislative solution to this dilemma. It closes the loophole by making two main changes.

First, it clarifies that private financial gain does include barter; that is, it does include situations where illegal copies are traded for items of value such as other copyrighted works.

Second, it redefines criminal infringement to include willful infringement by reproduction or distribution, including by electronic means that lacks a commercial motive, but does have substantial commercial effect.

The Copyright Office supports the proposed clarification of financial gain where definition is important because it has become common, for example, for electronic bulletin boards to employ bartering systems where users contribute pirated copies of computer software

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 9 1999

in exchange for the ability to download illegal copies or the ability to get illegal copies of other software.

The Office also supports the goal of the provisions which address damaging piracy motivated by non-commercial purposes.

While the existing commercial purpose requirement in a world of physical copies has served to limit criminal liability to piracy on a commercial scale, a new standard definitely is needed in the digital environment where significant economic damage can be caused without commercial purpose.

We are concerned, however, that certain aspects of the Bill could cause unintended negative consequences. In our view, it would be preferable to limit criminal liability for infringement without a profit motive to cases of willful infringement that threaten to cause substantial economic harm.

This result could be accomplished by incorporating the limits currently found in the proposed penalty provisions regarding time period, number of copies and retail values directly into the redefinition of criminal infringement. This would leave no doubt that minor, isolated instances of willful infringement would not inappropriately be subject to criminal liability.

Concern has also been expressed about the impact on libraries, universities and other non-profit organizations. Some have suggested that the proposed language, even as limited as we suggest, might expose these organizations inappropriately to the risk of criminal liability since the retail value limits could easily be surpassed.

Much of this concern, however, should be allayed by the requirement that infringement be willful. The courts have consistently held that it is not enough for the defendant in a criminal case to have had an intent to copy the work. He must have acted with knowledge that his actions constituted copyright infringement.

That is the reason non-profit organizations that implement a conscientious copyright policy should not be subject to the threat of criminal sanctions. In particular, if such an organization believes in good faith that its copying is permissible, as a fair use or under Section 108 or any other provision of the copyright law, it would not be acting willfully.

Congress may wish to consider putting—or you may wish to consider confirming this interpretation in the legislative history. However, if these institutions can identify specific situations where the Bill could create an inappropriate risk of criminal liability, the Copyright Office would be pleased to addressing your concerns.

And so we support the enactment of H.R. 2265 with minor revisions. It will close the gap in the existing legal shields against piracy, particularly as piracy has evolved on the Internet.

I thank you for the opportunity to testify, and I would be pleased to answer any questions.

[The Statement of Ms. Peters follows.]

PREPARED STATEMENT OF MARYBETH PETERS, REGISTER OF COPYRIGHTS

H.R. 2265 would amend current law governing criminal copyright infringement to cover willful piracy that may cause serious commercial harm despite the infringer's lack of a profit motive. The Copyright Office supports the bill's purpose and approach, which will close a significant loophole that exists in current law. Although

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 10 1999

we have some concerns with respect to specific language in the bill, we are confident that they can be resolved.

Existing law provides that copyright infringement can be prosecuted criminally only where the infringement is done "willfully and for purposes of commercial advantage or private financial gain." 17 U.S.C. §506(a). Advances in technology have increased the potential for damage from copyright piracy, as it becomes easier and easier to make and distribute high quality copies without a major investment in equipment and facilities. In particular, the ease with which copyrighted works can be transmitted via the Internet makes it more likely that damaging copyright piracy will occur without a commercial motive on the part of the infringer.

The recent case of *United States* v. *LaMacchia* provides a clear example of the current law's shortcomings in the new digital environment, and the enforcement and deterrence problems caused by the lack of criminal penalties for deliberate and damaging noncommercial copyright piracy.

H.R. 2265 would also improve the existing criminal provisions for commercial piracy. The Copyright Office supports the proposed definition of "financial gain," which encompasses bartering systems and other nonmonetary compensation schemes commonly used by infringers on the Internet.

In addition, the Copyright Office supports the bill's goal of amending section 506 to make serious copyright piracy that lacks a profit motive subject to criminal penalties. A new standard is necessary to account for the damaging copyright piracy that can take place on the Internet without any commercial motive or profit. However, we have some concerns that the language as drafted might cause unintended negative consequences. We suggest incorporating the specific limitations regarding time period, number of copies and retail value, which the bill includes in the penalty provisions, directly into section 506 to make clear that criminal penalties apply to infringement without a commercial motive only where the infringement causes significant commercial harm. This should eliminate concerns that the legislation would criminalize minor, isolated instances of willful infringement.

We are confident that H.R. 2265, with the minor revisions suggested, will close the major loophole in current law and help to prevent copyright piracy, particularly as it has developed in the Internet context.

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to testify on this important piece of legislation, the "No Electronic Theft (NET) Act of 1997." The bill would amend the provisions of current law dealing with criminal liability for copyright infringement to cover willful piracy that may cause serious commercial harm despite the infringer's lack of a profit motive.

The Copyright Office supports the purpose and approach of the proposed changes. We agree with the sponsors of the bill that a significant loophole exists in current law, which permits deliberate and destructive piracy to escape criminal penalties where it is done for motives other than financial gain. In order to preserve legitimate markets for copyrighted works, it is critical, especially in the era of digital transmission, to close this loophole quickly. While we have some concerns with respect to specific language of the proposed changes, we are confident that these concerns can be resolved.

INTRODUCTION AND BACKGROUND

The Copyright Act provides for both civil and criminal liability for acts of copyright infringement. 17 U.S.C., Chapter 5. Infringement is a crime only where it is done "willfully and for purposes of commercial advantage or private financial gain." 17 U.S.C. §506(a). The penalties for criminal infringement, set forth in Title 18 of the U.S. Code, are determined by its extent: if the infringer has made, in any 180-day period, ten or more copies of one or more copyrighted works with a total retail value of $2,500, the crime is a felony entailing up to five years imprisonment and/or a fine of up to $250,000 for individuals and $500,000 for organizations. 18 U.S.C. §§2319(a), 3571(b). For cases not meeting this threshold, the crime is a misdemeanor, with the maximum penalty of imprisonment for up to one year and/or a fine of up to $25,000 for individuals and $100,000 for organizations. *Id.* §§2319(c), 3571(b). There is also an increased penalty for repeat offenders, authorizing a sentence of up to 10 years. *Id.* §2319(b).

This general approach to criminal liability dates back to the first criminal infringement provision in the copyright law, which required the infringement to be "willful and for profit." Act of January 6, 1897, 54th Cong., 2d Sess., 29 Stat. 481. The profit element was maintained in the 1909 Copyright Act, but was elaborated in 1976 to read "for purposes of commercial advantage or private financial gain." 17 U.S.C. §506(a). Although Congress did not explain the change, *see* H.R. Rep. 1476, 94th Cong., 2d. Sess. 163 (1976), courts have pointed out that the current lan-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 11 1999

guage conforms to judicial interpretation of the prior law's "for profit" requirement as covering infringers who intended to make a profit but did not actually do so. *See United States* v. *Cross*, 816 F.2d 297, 301 (7th Cir. 1987); *United States* v. *Moore*, 604 F.2d 1228, 1235 (9th Cir. 1979).

The damage from piracy has grown over the years as technology has developed, making it easier and easier to produce higher quality copies of copyrighted works in various formats. Copyright owners today lose substantial sums of money to piracy. The advent of digital technology has the potential to exacerbate greatly the impact of piracy, as it allows users to make multiple perfect copies in an instant, without requiring a major investment in physical manufacturing and distribution facilities. As it becomes easier to transmit large amounts of information quickly over the NII, it becomes easier for those without a commercial stake or profit motive—a disgruntled former employee, a dissatisfied customer, an Internet user opposed to the fundamental concept of copyright law—to inflict tremendous damage to the market for a copyrighted work. In contrast to the traditional analog world, substantial commercial harm may easily be caused by the act of a single person without a commercial aspect to the piracy itself. Moreover, for such infringers, civil remedies are less likely to serve as an effective deterrent and criminal sanctions may be needed to deter these individuals from causing serious harm to the value of copyrighted works.

The case of *United States* v. *LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), has drawn attention to current law's shortcomings. David LaMacchia, a student at the Massachusetts Institute of Technology described by the court as a "computer hacker," *id.* at 536, created and operated electronic bulletin boards on the Internet and encouraged users to upload and download copies of popular copyrighted commercial software. The illegal copying that took place on the bulletin boards resulted in alleged losses to the copyright owners of over one million dollars. Because LaMacchia lacked a commercial motive, however, the government charged him with wire fraud rather than criminal copyright infringement. *Id.* at 541–42. The court dismissed the indictment, holding that copyright infringement can only be prosecuted under the Copyright Act. *Id.* at 545 (relying on *Dowling* v. *United States*, 473 U.S. 207 (1985)).

LaMacchia demonstrates that the lack of criminal penalties for willful, noncommercial infringement has become a significant loophole in the digital environment. The court itself decried this loophole, expressing frustration with the confines of section 506(a):

> [O]ne might at best describe [the defendant's] actions as heedlessly irresponsible, and at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values. Criminal as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. . . . But, it is the legislature, not the Court which is to define a crime, and ordain its punishment.

Id. at 545 (quotations omitted).

H.R. 2265 responds to the court's call for a legislative solution to its dilemma. The bill would close the loophole in current law by making two main changes. First, it clarifies that the "private financial gain" element of criminal infringement includes barter—that is, situations where the illegal copies are traded for items of value such as other copyrighted works, not only where they are sold for money. Second, it redefines criminal infringement to include willful infringement by reproduction or distribution, including by electronic means, that lacks a commercial motive but has a substantial commercial effect.

ANALYSIS

A. Definition of "Financial Gain"

Section 2(a) of the bill would introduce a new definition in section 101 of the Copyright Act for the term "financial gain." Under the current section 506(a), the standard for criminal liability is that the infringer acted "willfully and for purposes of commercial advantage or private financial gain." The new definition of "financial gain" would clarify that the term "includes receipt of anything of value, including the receipt of other copyrighted works." This language ensures that criminal liability will not turn on the technicality of whether the infringing copies were sold for money, as opposed to other valuable benefits.

The Copyright Office believes that the proposed clarification is desirable. The new definition will be particularly important in protecting copyright owners from piracy on the Internet, where a multitude of economic models have developed to compensate infringers for their illegal copies. It has become common, for example, for electronic bulletin boards to facilitate bartering systems where users contribute copies of infringing software in exchange for the ability to download copies of other soft-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 12 1999

ware. *See, e.g., Sega Enters. Ltd.* v. *MAPHIA,* 948 F. Supp. 923, 927–28 (N.D. Cal. 1996); *LaMacchia,* 871 F. Supp. at 536.

B. Substitution of Commercial Impact for Commercial Purpose

Other sections of the bill allow criminal liability for willful infringement to be based on the commercial impact on the copyright owner rather than the commercial purpose of the infringer.

Section 2(b) of the bill renumbers the existing criminal infringement provision in section 506(a) as subsection 506(a)(1), and adds a new subsection 506(a)(2). Under the new subsection, any person who infringes a copyright "willfully . . . by the reproduction or distribution, including by electronic means, of 1 or more copies, of 1 or more copyrighted works" is subject to the criminal penalties set forth in Title 18. The core of this subsection is its omission of any requirement of commercial purpose or financial motive. In addition, it makes explicit that reproduction and distribution of electronic copies via the Internet can qualify for criminal sanctions.

The bill also revises section 2319 of Title 18 to set forth the penalties for violation of the proposed new subsection. Under the revisions, the criminal infringement would be a felony if the offense involves the copying or distribution, in any 180-day period, of ten or more copies of one or more copyrighted works with a total retail value of $5,000. *See* H.R. 2265, § 2(d) (adding new section 2319(c) to Title 18). The maximum sentence is up to 3 years in prison and/or a fine of up to $250,000 for individuals and $500,000 for organizations (the bill does not amend the existing fine amounts found in 18 U.S.C. § 3571). Repeat felony offenders could receive a sentence of up to 6 years. A less extensive violation of section 506(a)(2) would be a misdemeanor, with the maximum sentence of up to one year in prison and/or a fine of up to $25,000 for individuals and $100,000 for organizations. *See* H.R. 2265, § 2(d) and 18 U.S.C. § 3571.

As discussed above, the Copyright Office supports the goal of the proposed revisions in addressing damaging piracy that is motivated by non-commercial purposes. While the existing "commercial purpose" requirement, in the the world of physical copies, has served to limit criminal liability to piracy on a commercial scale, a new standard is needed in the digital environment, where significant economic damage can be caused without a commercial purpose.

We are concerned, however, that certain aspects of the language of H.R. 2265 as drafted could cause unintended negative consequences. Because of the placement of all the factors delineating the extent of the infringement in the penalties section in Title 18, the structure of the bill indicates that willful infringement through reproduction or distribution of a single copy of a copyrighted work could lead to criminal liability. While the more serious cases listed in Title 18 would constitute felonies, cases of less severity appear to qualify as misdemeanors.

In our view, it would be preferable to limit criminal liability for infringement without a profit motive to cases of willful infringement that threaten to cause substantial economic harm. When Congress last revised criminal penalties for copyright infringement, the legislative reports made clear that *de minimis* copying would not be subject to the new criminal penalties. *See* H.R. Rep. No. 102–997, 102d Cong., 2d Sess. 6 (1992). At that time, the House Judiciary Committee stated that the new felony provisions would not apply to "children making copies for friends as well as other incidental copying of copyrighted works having a relatively low retail value." *Id.* We believe a similar distinction is appropriate here.

This result could be accomplished by a change in drafting technique. We would suggest incorporating directly into section 506(a)(2) the limits currently found in the proposed penalty provisions regarding time period, number of copies and retail value. This approach would make clear that the new criminal provisions are limited to situations like *LaMacchia,* where the infringer's conduct substantially damages the market for the copyrighted works. The definition of the criminal conduct itself would then contain limitations—requiring the conduct to take place within a 180-day period and involve 10 or more copies of works worth $5,000 or more—that would leave no doubt that minor, isolated instances of willful infringement would not inappropriately be subject to criminal liability. The bill already takes similar precautions in this area by increasing the current felony "retail value" threshold for commercial piracy from $2,500 to $5,000. *See* section 2(d)(1).

Concern has also been expressed about the impact of the bill on libraries, universities and other nonprofit organizations. Some have suggested that the proposed language, even if limited as proposed above, might expose these organizations inappropriately to the risk of criminal liability, since the retail value limits could easily be surpassed, particularly by large nonprofits.

Much of this concern should be allayed by the requirement that the infringement be "willful," given the interpretation that courts have given this term in the crimi-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 13 1999

nal context. The courts have held that it is not enough for the defendant in a criminal case to have had an intent to copy the work; he must have acted with knowledge that his conduct constituted copyright infringement. *See, e.g.,United States* v. *Cross,* 816 F.2d 297, 300 (7th Cir. 1987) and *United States* v. *Moran,* 757 F. Supp. 1046 (D. Neb. 1991). In *Cross,* the Seventh Circuit upheld the following jury instruction for determining willfulness under the criminal provision of the Copyright Act:

> '[W]illfully' as used in the statute means the act was committed by a defendant voluntarily, with knowledge that it was prohibited by law, and with the purpose of violating the law, and not by mistake, accident or in good faith.

816 F.2d at 300.

In *Moran,* the defendant was charged with criminal infringement for his practice of making backup copies of the videotapes he purchased for his video rental store. The court held that the "willful" element of criminal copyright infringement was similar to that in federal criminal tax statutes, and thus requires a "voluntary, intentional violation of a known legal duty." *Id.* at 1049 (citing *U.S.* v. *Cheek,* 111 S.Ct. 604, 610 (1991)). The court therefore held that because the defendant believed, albeit incorrectly, that he had a right to make such copies, he could not be convicted of criminal infringement. *Id.* at 1051–52.

Thus, libraries and other nonprofit organizations that implement a conscientious copyright policy should not be subject to the threat of criminal sanctions under H.R. 2265. In particular, if such an organization believes in good faith that its copying is permissible as fair use or under section 108 or another provision of the Copyright Act, it would not be acting willfully. In order to confirm this interpretation, the legislative history could refer to the case law described above. To the extent that nonprofits may identify specific situations where the bill could create an inappropriate risk of criminal liability, the Copyright Office would be pleased to assist in developing language to meet their concerns while maintaining the intended purpose of the legislation.

The Copyright Office has one additional technical suggestion about the language of the bill. We recommend that the phrase "copies" that appears both in section 506(a)(2) and in section 2319(c) of Title 18 be expanded to read "copies or phonorecords," in order to cover all forms of material objects in which copyrighted works may be embodied. *See* definitions of "copies" and "phonorecords" in 17 U.S.C. § 101.

CONCLUSION

The Copyright Office supports enactment of H.R. 2265, with the minor revisions suggested. The bill would close a gap in existing legal shields against the piracy of copyrighted works, particularly as piracy has evolved into different forms in the Internet context.

Mr. COBLE. Thank you, Ms. Peters. I failed to mention earlier when I asked you all to try to confine your comments to five minutes, be assured—I say to the witnesses, your written testimony will not casually be discarded and tossed away. It will be carefully and thoroughly and deliberately examined.

So just because we are holding you to five minutes, do not think that your written testimony is going to be cast aside.

Mr. Di Gregory.

STATEMENT OF KEVIN V. DI GREGORY, DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. DI GREGORY. Good morning, Mr. Chairman and members of the Subcommittee. Thank you for this opportunity to describe the Department of Justice's enforcement of the criminal laws protecting copyright and to express the Department's strong support for the goals of H.R. 2265, the No Electronic Theft Act.

Intellectual property is one of this nation's most important resources, and with the help of Congress, the Department will ensure that the theft of copyright is vigorously prosecuted as we move further into the digital age.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 14 1999

Copyrighted goods, as has been already noted, can be illegally distributed, either physically or electronically. When distributed physically, copyrighted works are illegally reproduced here or abroad in a factory, and the pirated goods are sold to wholesalers, and then, in turn, to retailers, who sell the goods on the street.

One feature of this model of distribution is that the sale of goods on the streets is highly visible, making it more likely to attract the attention of law enforcement. Once the crime problem is targeted, the nature of the distribution scheme permits law enforcement to infiltrate the organization by obtaining the cooperation of the retailer to make a case against the wholesaler, and then use the cooperation, perhaps, of the wholesaler to make a case against the factory owner.

Through this process, an entire distribution scheme can be shut down, resulting in the seizures of a substantial number of illegally copied works.

To an ever-increasing extent, however, copyrighted works are being distributed electronically. This is a significant problem because computers that can easily copy and transmit digital information are relatively inexpensive.

Moreover, with digital copies, there is no deterioration in quality when second and third generation copies are made.

Accordingly, computers can illegally distribute copyrighted products around the world in the space of a few minutes.

At present, computer software companies are suffering the most at the hands of these copyright pirates, but as technology is permitting different types of work to be easily digitized and copied, other industries are being affected.

For example, the music industry is now beginning to suffer serious losses, and within a few years, the movie industry will find its products vulnerable to computer theft.

Pirates who operate electronically are often organized in gangs. Many pirate organizations operate through bulletin board services, or BBS's; that is, a computer or several computers often located in someone's home and reachable by customers or subscribers through telephone lines or computer modems.

Some of these BBS's operate by selling membership. Others operate on a trade or barter basis, requiring prospective members to contribute valuable software to the BBS.

These BBS's offer their membership hundreds of different programs, including expensive software from both large and small companies, and may even include software in versions not yet available to the general public.

Technology is also offering many new methods for distributing copyrighted works online.

Pursuing copyright pirates who operate in cyberspace presents different challenges for law enforcement than does combatting the illegal, physical distribution of copyright goods.

Electronic copyright violations are easy to overlook because rather than taking place openly on the streets, they take place hidden in cyberspace. Even when computer copyright violations are targeted, the lack of a vertical distribution scheme makes it difficult for a single case to noticeably impact the amount of copyrighted material available through illegal channels.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 15 1999

Finally, it is important to note that while a tangible distribution of copyrighted goods can be investigated by any law enforcement agent, computer violations require technically adept agents, who are in short supply.

Despite these formidable problems, the Department of Justice has made great strides for addressing the difficulties associated with electronic theft of copyrighted products.

We hope that by bringing the criminal laws to bear on some of the worst offenders, we will deter others.

One of the most important initiatives that we have taken is creating, in 1996, the computer crime Intellectual Property section within the Criminal Division, and one of the section's top priorities has been training Federal investigators and prosecutors.

We have recently published in May of this year, 175 page manual entitled, "Federal Prosecution of Violations of Intellectual Property Rights, Copyrights, Trademarks and Trade Secrets." This manual has been distributed to each of the 93 United States Attorney's offices and is available online.

The Computer Crime and Intellectual Property Section and U.S. Attorney's Offices around the nation have also been investigating and prosecuting copyright cases with increasing frequency. The FBI has made intellectual property protection one of its national crime priorities.

The Department strongly supports the goals of H.R. 2265. The *LaMacchia* decision holding that criminal statutes do not reach not-for-profit illegal distribution of copyrighted goods has impeded the Department's ability to prosecute copyright pirates in instances where clear proof of motive has been lacking.

NET would fix this statutory hole by creating a new provision that would criminalize willful infringement, even where there is no profit motive.,

We do have some concerns about H.R. 2265 in that it may sweep too broadly. These concerns, we believe, are easily remedied, and we are confident that we will be able to work with the Subcommittee to fine tune this particular provision.

In short, NET would give law enforcement the statutory tools we need to combat copyright crime. We look forward to working with the Subcommittee on this important matter.

And as a final note, Mr. Chairman, if I may say both you and Mr. Frank noted this in your opening statements. I think it is important that, as we proceed through this hearing, that we focus on the fact that we are talking about criminal activity and that we are talking about stealing, and we are talking about the impact of that theft on the victim and also the impact of that theft on the prosecutor; that is to say that we should also focus on the prosecutor's decision-making process with respect to these thefts, recognizing that these kind of thefts, in many ways, are no different than other thefts in that the prosecutor's job is simply to decide whether or not someone either intended to steal or someone wanted to aid someone who was intending to steal.

[The Statement of Mr. Di Gregory follows:]

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 16 1999

PREPARED STATEMENT OF KEVIN V. DI GREGORY, DEPUTY ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. Chairman and members of the Subcommittee: Thank you for this opportunity to describe the Department of Justice's enforcement of the criminal laws protecting copyright, and to express the Department's strong support for the goals of H.R. 2265, the "No Electronic Theft (NET) Act." Intellectual property is one of this nation's most important resources, and with the help of Congress, the Department will ensure that theft of copyright is vigorously prosecuted as we move further into the digital age.

A. Copyright Protection in the Digital Landscape

The advent of powerful and inexpensive computing is bringing many changes to the way that copyrighted works are being illegally distributed, and hence to the methods that law enforcement uses to combat copyright piracy. Traditionally, copyrighted works—including books, records, and audiotapes—have been illegally reproduced here or abroad in a factory. The pirated goods are sold to wholesalers, and then in turn to retailers, who sell the goods on the street. In this type of distribution scheme, the damage to copyright owners, while substantial, is subject to certain technological limits. That is because the equipment necessary to reproduce the works in bulk is relatively expensive to purchase, and second generation products (*i.e.,* copies of copies) are either impossible for the customer to make (for records and compact disks), or else suffer in quality (for audio and video cassettes).

Another feature of this model of distribution is that the sale of goods on the street is highly visible, making it likely to attract the attention of law enforcement. Once the crime problem is targeted, the nature of the distribution scheme permits law enforcement to infiltrate the organization by obtaining the cooperation of the retailer to make a case against the wholesaler, and then use the cooperation of the wholesaler to make a case against the factory owner. By this process, an entire distribution scheme can be shut down, resulting in the seizure of a substantial number of illegally copied works.

This illegal distribution of copyrighted goods through tangible means continues to present a pressing problem for copyright owners, particularly for producers of books, movies, music, and computer software.[1] Accordingly, law enforcement continues to concentrate a great deal of attention on investigating and prosecuting these copyright pirates. To an ever-increasing extent, however, copyright piracy is being carried out through computers. Anything capable of being digitized—that is, reduced to a series of zeros and ones—is capable of being transmitted easily from one computer to another. Pirates have used this capability of the computer to steal vast amounts of copyrighted material, and illegally transfer it to others.

Up to now, it has been computer software companies who have suffered the most at the hands of the pirates. As technology is permitting different types of works to be easily digitized and copied, other industries are being affected. For example, the music industry is now beginning to suffer serious losses from computer pirates. And within a few years, the movie industry will find its products vulnerable to computer theft.

Pirates who operate electronically are often organized in gangs. Many pirate organizations operate through "Bulletin Board Services," or BBS's: a computer or several computers often located in someone's home, and reachable by customers or subscribers through telephone lines and computer modems. Some of the BBS's offer pirated software—called "warez"—exclusively. Others offer legitimate services, such as discussion groups, or a platform for trading "shareware" (software not covered by copyright), and contain pirated material on parts of their BBS's accessible only through a password.

Some of these BBS's operate by selling memberships. Others operate on a trade or barter basis, requiring prospective members to contribute valuable software to the BBS. In either event, the member is permitted to access and copy copyrighted software from the BBS. These BBS's often offer hundreds of different programs, including expensive software from large and small companies, and may even include software in versions not yet available to the general public. The unauthorized distribution of valuable works by pirates has almost destroyed some software developers and seriously injured countless others.

Although distributing software through BBS's is the method of choice for present-day computer pirates, other computer network services are providing new means for

[1] Machines capable of copying software onto compact discs now retail for approximately $600; these machines are often used to transfer thousands of dollars of illegally copied software programs onto a single disk, which is sold to the user for about $20.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 17 1999

copyright crime to occur. For example, there are certain electronic "chatrooms" devoted to the discussion of the availability of illegally copied programs. Programs can be sent through e-mail or, more typically, through World Wide Web sites or other programs that allow for the rapid exchange of digital information.

Pursuing copyright pirates who operate in cyberspace presents different challenges for copyright owners and for law enforcement than does combating the illegal physical distribution of copyrighted goods. First, unlike the equipment necessary to make large-scale physical copies of tapes and disks, computers than can easily copy digital information are relatively inexpensive. Second, with digital copies, there is no deterioration in quality when second or third generation copies are made. Accordingly, a copyrighted product can be placed on a BBS or website and copied by hundreds of people. Those people can then redistribute the copy to others, illegally spreading the product around the world in the space of a few minutes.

For law enforcement, electronic copyright violations are easy to overlook, because, rather than taking place openly in physical space, they take place hidden in cyberspace. Even when computer copyright violations are targeted, the lack of a hierarchical distribution scheme makes it difficult for a single case to make a noticeable impact on the amount of copyrighted material available through illegal channels: the software no longer available from one BBS can simply be found elsewhere. Finally, it is important to note that while the tangible distribution of copyrighted goods can be investigated by any law enforcement agent, computer violations require technically adept agents. These agents are in short supply, despite the efforts of federal law enforcement agencies to hire and train agents to deal with computer crime. Even when investigative agencies have such resources, they are often needed to investigate other computer crimes, such as attacks on the confidentiality, integrity and availability of computer systems and data.

B. Law Enforcement's Approach to Computer Copyright Theft

Despite these formidable problems, the Department of Justice has made great strides toward addressing the difficulties associated with electronic theft of copyrighted products. We hope that by bringing the criminal laws to bear on some of the worst offenders, we will deter others from engaging in these illegal activities.

One of the most important initiatives that the Department has undertaken in this area is creating, in 1996, the Computer Crime and Intellectual Property Section (CCIPS) within the Criminal Division. As its name indicates, CCIPS is responsible for coordinating both the Department's policies regarding computer crime and the enforcement of criminal laws protecting intellectual property. CCIPS is headed by Scott Charney, a highly-regarded expert in these fields. The Section has particular expertise in the area this Subcommittee is considering today: computer-based copyright theft.

One of the Section's top priorities has been training federal investigators and prosecutors. In May of this year, CCIPS published a 175-page manual entitled, "Federal Prosecution of Violations of Intellectual Property Rights: Copyrights, Trademarks and Trade Secrets." The Manual has been provided to each of the 93 U.S. Attorney's Offices and is available on line.[2] The Manual provides agents and prosecutors with a detailed resource for undertaking prosecutions in the law.

In addition, CCIPS works with a "Computer and Telecommunication Coordinator" (CTC) in each U.S. Attorney's Office. The CTC is a prosecutor specially designated by the U.S. Attorney as the expert in that district on high-tech crime, and is given specialized training in both computer crime and intellectual property protection.

CCIPS also provides training to state and local agents and prosecutors in a variety of settings. Finally, CCIPS is active in training law enforcement officials from other nations. Section attorneys have traveled to Russia, Egypt, and many other countries to give guidance to our counterparts there, and regularly instruct foreign officials visiting the United States on U.S. laws and techniques for combating copyright piracy. These efforts are particularly important to the United States because many of the products being illegally copied abroad are produced by U.S. companies, and because computers make it easy to send such pirated works across international boundaries.

CCIPS and U.S. Attorneys' Offices around the nation have also been investigating and prosecuting copyright cases with increasing frequency. The Department's enlarged focus on the issue has been matched by the investigative agencies assigned to this area: the Federal Bureau of Investigation and the U.S. Customs Service.

The FBI has made intellectual property protection one of its national crime priorities. Two of the notable operations that have recently arisen from the FBI's

[2] The Manual can be found on the Computer Crime Section's Web page, http//www.usdoj.gov/criminal/cybercrime.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 18 1999

stepped-up enforcement efforts are "Operation Cyber Strike" and "Operation Counter Copy."

Operation Cyber Strike was an eight-month undercover investigation of pirate BBS's, run out of the FBI's International Computer Crime Squad in San Francisco. Earlier this year, search warrants were executed on ten large pirate BBS's around the country, receiving publicity from both the mainstream press and (perhaps more important for deterrence purposes) the pirate community. That investigation is continuing. Operation Counter Copy, while not focused exclusively on computer piracy, brought together a number of the FBI's cases involving criminal copyright and trademark cases. The operation resulted in thirty-five indictments in April, as well as eight guilty pleas.

The U.S. Customs Service is also actively involved in protecting against the illegal importation of infringing products, and seizes $45 million in such products annually. Recently, an undercover effort aimed at the importation of "bootleg" compact disks—recorded without the permission of the recording artist—resulted in a 39-count indictment and subsequent guilty pleas by fifteen defendants, as well as the seizure of 800,000 CD's worth over $20 million.

C. The No Electronic Theft (NET) Act

As we look toward the future, it is clear that the effort to deter electronic theft would be greatly aided by new legislation. The Department believes that H.R. 2265, the No Electronic Theft (NET) Act, contains a number of important provisions that will help the Department protect copyright in the digital age. We commend the sponsors of the bill,[3] and strongly support legislation on this subject.

One of the key provisions of NET is the creation of a new criminal offense to cover the unauthorized distribution or reproduction of copyrighted materials, regardless of whether the distributor was trying to profit from the activity. The provision would cover a gap in the current criminal statute that was exposed by the District Court's dismissal of an indictment in *United States* v. *LaMacchia,* 871 F. Supp. 535 (D. Mass. 1994).

In *LaMacchia,* an MIT student operated a computer bulletin board system over the Internet that allowed anyone with a computer and modem to send to the board or acquire from the board copyrighted software programs. His actions caused an estimated loss to copyright holders of over $1 million during the six-week period the system was in operation. The student could not be charged with violation of the criminal law protecting copyright, 17 U.S.C. §506, because he was not acting "for commercial purpose or private financial gain," an element of the criminal copyright offense. Instead, he was charged with conspiracy to commit wire fraud, 18 U.S.C. §1343.

The district court dismissed the indictment, because it viewed the copyright law as the exclusive remedy for protecting intellectual property rights from this kind of theft, even while recognizing that the current copyright law fails to cover this conduct. The Court explicitly invited Congress to remedy this gap in the law:

> This is not, of course, to suggest that there is anything edifying about what *LaMacchia* is alleged to have done. If the indictment is to be believed, one might at best describe his actions as heedlessly irresponsible, and at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values. Criminal as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution. But, "[i]t is the legislature, not the Court which is to define a crime, and ordain its punishment." [citation omitted].

871 F. Supp. at 545.

The *LaMacchia* decision has impeded the Department's ability to prosecute copyright pirates in instances where clear proof of a profit motive has been lacking. NET would fix this statutory hole by creating a new provision, to be codified at 17 U.S.C. §506(a)(2), which would criminalize willful infringement, even when there is no profit motive, and establish a three-year felony for reproducing or distributing, during any 180-day period, ten or more copies of one or more copyrighted works which have a total retail value of more than $5,000.

---

[3] We similarly commend Senators Leahy and Kyl, the sponsors of a similar bill in the Senate. That bill is S. 1044, and is called the Criminal Copyright Improvement Act of 1997.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 19 1999

We do have some concerns that H.R. 2265 may sweep too broadly.[4] These concerns are easily remedied, however, and we are confident that we will be able to work with the Subcommittee to fine tune this particular provision.

Filling the gap caused by the *LaMacchia* decision is only one of the benefits that this bill brings to criminal enforcement of the copyright laws. The bill has a number of other important provisions. They include:

Establishing a recidivist provision, which raises penalties for second or subsequent felony criminal copyright offenses;

Extending the statute of limitations from three to five years, bringing it in line with most other criminal statutes;

Clarifying that the term "financial gain" includes the receipt of anything of value, including the receipt of other copyrighted works, to ensure that pirate operations that require barter rather than cash are covered;[5]

Clarifying that "reproduction or distribution" includes electronic as well as tangible means;

Extending victims' rights by allowing the producers of pirated works to provide a victim impact statement to the sentencing court; and

Directing the Sentencing Commission to amend the Sentencing Guideline for copyright and trademark infringement to allow courts to impose sentence based on the retail value of the good infringed upon, rather than the often lower value of the infringing good.

In short, NET would give law enforcement the statutory tools we need to combat copyright crime. We look forward to working with the Subcommittee on this important matter.

I would be pleased at this time to answer any questions you may have.

SUMMARY

The increasing prevalence of copyright theft through electronic means is creating new challenges for law enforcement. Computer pirates organized in gangs illegally distribute copyrighted software and other works at rapid speed, causing untold harm to the producers of such works.

The Department of Justice has responded to this challenge by creating a new Section in its Criminal Division devoted to protecting against computer crime and intellectual property theft. That Section is training federal and state prosecutors and agents on the techniques of combating this type of crime, and training foreign officials to help ensure that copyright is protected world-wide. The Department and the law enforcement agencies that protect copyright—the Federal Bureau of Investigation and the U.S. Customs Service—are placing increasing emphasis on investigating and prosecuting thefts of intellectual property, whether by physical or electronic means.

The Department is highly supportive of the goals of H.R. 2265. The bill would allow the Department to prosecute large-scale theft of copyright, even when the perpetrator was not acting out of a profit motive. The bill would also accomplish a number of other important objectives, including establishing a recidivist provision; extending the statute of limitations; clarifying that "financial gain" includes the receipt of other copyright works; clarifying that "reproduction or distribution" includes electronic as well as tangible means; extending victims' rights by permitting victim impact statements in intellectual property cases; and directing the Sentencing Commission to reflect more accurately the harms caused by copyright piracy by imposing sentence based on the retail value of the good infringed upon, rather than the value of the infringing product.

We look forward to working with the Subcommittee on this important piece of legislation.

---

[4] H.R. 2265 permits misdemeanor penalties to be imposed for willful infringement by reproducing or distributing one or more copies of one or more copyrighted works, regardless of their retail value. The bill prescribes three-year felony penalties for reproducing or distributing, during any 180-day period, 10 or more copies of one or more copyrighted works, which have total retail value of more than $5,000.

S. 1044, by contrast, imposes a misdemeanor criminal penalty for non-commercial willful infringement *only* if ten or more copies of one or more copyrighted works are reproduced or distributed during any 180-day period *and* if the total retail value of the works or copies is $5,000 or more. Felony penalties would become available in non-commercial cases if the total retail value of the copied works exceeded $10,000.

[5] We would be happy to work with the Subcommittee to formulate language to ensure coverage of pirates who provide copyrighted products with the *expectation* of receiving anything of value, even if they have not yet received that thing of value.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 20 1999

Mr. COBLE. I thank you, and your written testimony, as supported your oral testimony today, indicates to me that each of you is supportive of Mr. Goodlatte's Bill, but you may want it tweaked maybe here or there.

Ms. Peters, would you recommend defining the term, "willful," in the statute, or do you believe that report language and existing case law on the subject will suffice to protect libraries, universities and other non-profit organizations?

Ms. PETERS. I would defer to what Congress decided in 1992. In 1992, when Congress amended the law to add additional criminal penalties to cover all types of works, the question was whether or not willful should be defined in the statute. And Congress, at that time, decided not to include that and that the courts would continue to define it in the way that it had consistently been applying it in the past.

So I basically think that you could handle it through legislative history and the courts and not necessarily have to put it in the statute. And that was the decision that was reached in 1992.

Mr. COBLE. This—let me say it a different way. This might be difficult to handle precisely, but what percentage of computer users who infringe actually know what they are doing?

In other words, how many infringers know they are breaking the law? And the reason I ask this, folks, I have some empathy with people who break the law, but who do it innocently, who lack intent.

Do you all have a read on that?

Ms. PETERS. I cannot answer that question. Certainly my employees know about it.

I think maybe there is a significant lack of knowledge, but not with the people that we are talking about because they are willful infrigners.

I think that education is a critical part, and I know that there are a lot of people, including the Copyright Office, whose aim is to get education at the lowest possible level, so when people sign onto a computer, they learn the rules of the road and learn about intellectual property.

But hearing you talking about willful, the ones we are talking about are people who do know they are infringing.

Mr. COBLE. Each of you pretty clearly at least suggests in your written testimony that you believe the contents of H.R. 2265 may, at different points, constitute overreach.

How about elaborating a little more in detail how we might improve on that if, in fact, Mr. Goodlatte is overreaching.

Ms. PETERS. We—you can go.

Mr. DI GREGORY. I was going to actually—I had a chance to look at Ms. Peters testimony prior to coming here, and I think in her written testimony, she proposes a rather interesting and probably useful solution.

Ms. PETERS. What we basically said was that the way that it reads now, it talks about one or more works and one or more copies, and that if you take what is in the penalty section, which makes it clear that you have to have ten or more copies whose value is $5,000 in the 180-day period, and you put that in the defi-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 21 1999

nition, you will, in fact, take away the one individual who sends a song to his friend on e-mail.

Mr. DI GREGORY. And from our perspective, I am not sure that we—that we want to be in a position to Federally prosecute that particular individual who decides to take that one piece of copyrighted material and send it to a friend or a relative. And I am not—and I do not know whether or not you all can answer that, whether or not it would be your intent to, again, Federally criminalize that type of activity when what we really want to deter clearly are those people who are engaged in willful, knowing violations of the law, whether for profit or not.

Mr. COBLE. The gentleman from Massachusetts, Mr. Frank.

Mr. FRANK. That seems to me to be a clear example of where we can get agreement on the concept, but then the implementation will be an issue. I have to read the testimony of Mr. Nimmer about the Telephone Association because I am not going to be—sure about his input.

I mean we would have to ask both of you very well, because both of you would be involved in the enforcement of this.

Their fear is that the language here—I would assume the word, "distribution," say on line 12 of page 2 of the Bill, when it says, "by the reproduction or distribution, including by electronic means, of one or more copies," that a service provider would be criminally liable simply because some infringer used the service.

Now, obviously, that is not what we would want to see any of this—when we—I assume that we agree on that, that we do not want to see that.

So if that is the case, what is your view of the argument and is there anything that we could do that would make it clear that that is not what we mean?

Ms. PETERS. Can I just start with saying that I think it has no impact on online service provider liability. Today, under the copyright law, you are only criminally liable for aiding and abetting only if you willfully associate with the criminal venture, you willingly participate in it and you willingly seek to make it succeed. So you have to do something that aids and abets that activity.

Mr. FRANK. Well, my concern is that someone might interpret making it physically possible for everybody to read this as aiding and abetting. And I certainly would not want to think of my service provider as trying to deter me or retard me.

Ms. PETERS. They can answer how they would do that, but certainly, there is a knowledge standard, and you cannot be just a passive carrier. You have to do more.

Mr. COBLE. What you are saying is if that is the current state of the law that passive carriers are protected——

Ms. PETERS. Absolutely.

Mr. FRANK [continuing]. And that nothing in here changes that?

Mr. Di Gregory.

Mr. DI GREGORY. I do not think anything in here changes that, either.

In fact, I mean going back to the point that I made at the very end of my statement, I think what—what we are looking to do in enforcing the law is to decide whether or not somebody had the

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 22 1999

criminal intent to steal or decide whether or not somebody had the criminal intent to aid or abet that——

Mr. FRANK. Well, I mean, one way we might be—if we agreed that—if their suggestion—and I will ask Mr. Nimmer when he comes forward—is that we have somehow here changed the standard that now obtains for a provider, then obviously, we are going to reach that later on. But would there be harm in adding a sentence or two that said, "Nothing in this Act is intended to change the current law regarding the liability of the service provider."

Ms. PETERS. Mr. Frank, what I was saying is, that is very similar to the argument that I was raising with regard to libraries and other institutions who would have computers in their institutions and a student would come in, and unless they actively aided and abet—and my suggestion was that, in the legislative history, you could basically put out the parameters of willful.

Mr. FRANK. Yeah. But you got to remember—I appreciate that little bit of history, but we do confront, at least in the presence of Justice Scalia, a man with at least in his capacity as a Supreme Court Justice, a man with a limited attention span; that is——

Ms. PETERS. Well, he certainly——

Mr. FRANK. He will direct his attention to the words of the statute and nothing else.

Ms. PETERS. Exactly. I was just going to say this.

Mr. FRANK. So what about simply trying to find some language to put into the statute—when we go through this—I have to say sometimes raise these issues not because they are concerned about them, but because they do not like the whole Bill and they do not want to say so. But I do not think that is what the phone company is doing here.

And when people are not raising an issue like that and you think that it may not be the real issue, the best way to deal with it is, in fact, to concede that point so if they have an underlying agenda——

And I would say, I want to put a computer key on the keyboard down in the Legislative Council office that says, in effect, "This Bill does not do what this Bill does not do." And I would want to put a clause like that in here saying, "Nothing in this legislation changes those things."

Would there be any reason not to do that, and would that not be a shoo in, Mr. Di Gregory?

Mr. DI GREGORY. I think that I had a very brief opportunity to look at Professor's Nimmer's testimony. I think that this is certainly an issue that we would be glad to discuss with the Committee with respect to when we go from—because I am concerned about the impact about specifically defining, "willfulness," for the purposes of this statute and——

Mr. FRANK. There are two separate issues here, right, and one is willfulness, but there was at least, in our—a definable issue which is they do not want, by this statute—they do not want a broader definition of willful to somehow change what would be the liability of the online service provider.

And maybe we should just explicitly say we are not here trying to change whatever that is because we are going to deal with it later.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 23 1999

And people sometimes change that unnecessarily. I think there is one principal, because there is going to be a lot of fears we are dealing with, and I hope we accept this throughout.

Legislation is not literature. Redundancy is not a problem. The amount of paper we are using is diminimus.

And if people are uncertain, there is nothing to be lost by simply being explicit.

And the fact that you think it already says that is no reason not to say it again, because it does not have other negative implications.

So I would ask you many times to explain—to address that question about how do we deal with the feelings that are expressed in Mr. Nimmer's testimony that someone might take this beyond where we intended it to go so we could then limit it to exactly what we wanted or as close to it?

Mr. COBLE. Thank you.

Mr. FRANK. Thank you.

Mr. COBLE. The gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. Di Gregory, how difficult is it to monitor this kind of electronic piracy?

Mr. DI GREGORY. I think you can monitor it through various investigative techniques. It is just—I think the most significant problem that we have is lack of resources in order to be able to monitor a great deal of it.

But there are literally hundreds of thousands of web sites, and it is rising at an enormous rate, so for every one that may be found in the active—in the act of giving out information that they are not supposed to, and I am sure that the vast majority of people who maintain web sites do not intend to infringe people's copyrights, but for every one that is, there may be a great many who are not detected.

Mr. GOODLATTE. What about the rate of recidivism of those who participate in these types of things?

Mr. DI GREGORY. I do not have any statistics for you on the rate of recidivism, but I suppose with respect to many of these pirates who are operating, when they are found out, it is probably not the first time they have done—engaged in the particular activity that they have engaged in.

Mr. GOODLATTE. Is there a problem with this within the Federal Government agencies themselves? Do you make any effort to deal with infringement?

Mr. DI GREGORY. I would have to get back to you on that because I am unaware of any efforts that we have any specific efforts that we have undertaken with respect to infringement.

Mr. GOODLATTE. OK. So you would not know, agency by agency, which one may have a serious problem with this, which ones may not?

Mr. DI GREGORY. No, I do not. I am sorry, but as I said, I can check on that for you.

Mr. GOODLATTE. We would welcome any information that you might have in that regard.

And Ms. Peters, we take note of your concern that we place in the actual Section 506 criminal offenses, the definition of what con-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 24 1999

stitutes an offense here, to make that clear. And we will certainly discuss with the other members of the Committee whether we think that is necessary to make that clear.

It certainly is not our intent, and I want to make it very clear that one person sending one item, however, contrary to the concept of intellectual property that might be, we are not out to create a law enforcement mechanism to deal with that. We are talking about people who are giving away wholesale amounts of pirated software.

Thank you, Mr. Chairman.

Mr. COBLE. The gentleman from California. I recognize you for five minutes.

Mr. BERMAN. Thank you, Mr. Chairman.

I am curious. Civil remedies against copyright infringement, is the issue of commercial gain an issue there?

I guess for damages, well, I do not know, the loss or the gain, is there a quick answer to that question?

Ms. PETERS. Well, there is willful infringement that has higher damages, and certainly, when you are talking about actual damages, and even with regard to statutory, you take into account commercial harm.

Mr. BERMAN. If someone has——

Ms. PETERS. Yes.

Mr. BERMAN [continuing]. LaMacchia——

Ms. PETERS. Right.

Mr. BERMAN [continuing]. Was there a basis here for holding him civilly liable for what he did, even though he could not be found criminally liable——

Ms. PETERS. Absolutely.

Mr. BERMAN. Because——

Ms. PETERS. Because he based it——

Mr. BERMAN [continuing]. He is not a——

Ms. PETERS. Basically he——

Mr. BERMAN [continuing]. Element of the——

Ms. PETERS [continuing]. Infringed the work, he would be subject to actual damages, and if you can prove the million dollars that was alleged and he had the money to pay it.

Mr. BERMAN. I am trying to understand Mr. Frank's issue. There is a law and now there is a bill dealing with the elimination of the for profit as the prerequisite to criminal culpability.

How does the issue of innocent reproduction or innocent distribution change by virtue of anything that Mr. Goodlatte is suggesting doing? Is distribution a new concept in Mr. Goodlatte's bill?

It does not exist in the existing law?

Mr. DI GREGORY. No. It is—I think it is—there is a clarification in the law to ensure that electronic distribution—electronic reproduction is included.

Ms. PETERS. So is the reproduction and distribution includes by electronic means.

Mr. BERMAN. So the fear that all of a sudden it will be somewhat easier to convict a willful infringer, because you will not have to prove commercial gain in some sense has no impact on the issue of—well, I guess the issue is whether it is a willfully distributes, and that is the same, and what Mr. Frank is suggesting, is there

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 25 1999

a way of insuring that there is nothing in the elimination of commercial gain standard that now impacts a distributor differently than he was impacted under—

Ms. PETERS. Right.

Mr. BERMAN [continuing]. Existing law.

Is that a fair——

Mr. FRANK. Are you talking now to me?

Mr. BERMAN. Yes.

Mr. FRANK. He is clarifying for me the fact that with the language, even if it does not have anything to do with that, it does not mean he is making—because you say all they are doing is relying on the commercial aspect. And I do not know any of the online service providers that distribute this stuff for free. They may ruin the commercial business.

So eliminating the commercial motive would not seem to implicate them anymore than they already are implicated now, but to say I do not mind a little reassurance, if that calms people down.

Mr. BERMAN. All right. That is what occurred to me. And I had another question, but I forgot it, so you can get back——

Mr. COBLE. I thank the gentleman from California.

Mr. Bono, for five minutes.

Mr. BONO. Thank you, Mr. Chairman. I just actually had the same concerns that Barney had, and they are kind of rolling out here. And if that is very clear, I think that that is the big issue.

I am concerned about otherwise protection of copyright. I could not be more for it. I think that intellectual property and technology is going to become the product of America, and it is becoming that way more and more.

And to have any loopholes in the theft of it is a big mistake for us because I think it takes the world market away from us. And I think that it is terrible economically.

So I am all for it. I would like to see it protected, and if it needs a little extra language and you are not concerned with that, maybe we could look at that so that everybody feels comfortable about it.

But I think that it is great that we are making this effort to protect intellectual property any way we can and copyrights any way we can. So I am——

Mr. COBLE. I thank the gentleman.

The gentlewoman from California is recognized for five minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

I am interested Ms. Peters, in your judgment that criminal penalties, if we are to attach them, should be reserved for cases where, on page 7, you say, "in willful infringement that would cause substantial economic harm"——

Ms. PETERS. Right.

Ms. LOFGREN. And the issues you have raised about fair use and libraries and schools.

Do you think that merely defining "willful," as you expressed in your testimony, either through legislative history or in the statute itself, is sufficient to protect non-profits, libraries, and schools in the fair use arena?

Ms. PETERS. What we said was we felt that that was enough. However, I do not—I live in a library, but I am not a librarian. And

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 26 1999

if they see specific instances that they think are problems, we would be glad to try to address those problems.

But, yes. We believe that the way that courts have continuously interpreted "willful" would end, we said, and if they have a policy that basically is a good copyright policy and they believe that they are operating under fair use that they cannot be held liable criminally.

Ms. LOFGREN. At least in my personal experience with schools and libraries, they are scrupulous. I mean really much more than ordinary citizens. They take the responsibility pretty seriously, which is good. They should.

I am wondering, Mr. Di Gregory, do you concur with Ms. Peters?

Mr. DI GREGORY. I think I would again go back to my earlier comment that what prosecutors are going to be looking for is whether or not they can establish that there was an intent to steal or that someone was aiding or abetting an intent to steal.

Ms. LOFGREN. I agree with that, but copyright law is and always has been a balance. We want to protect the intellectual property of the creator, and yet society has an interest in dissemination of ideas in intellectual property, as well, hence the fair use doctrine.

And so we need a strong right of fair use, even though, in fact, a prosecutor likely would not go in and prosecute the third grade teacher for making a back-up copy of the educational software.

So I was intrigued by your idea in terms of should there be—Ms. Peters' referenced in a different way the number of copies or——

Ms. PETERS. Well, actually, that is—it is just in the penalty part. And we just wanted to make it clear in the definition.

But I strongly believe that the willful standard that is there today would make it so that libraries and educational institutes who operate in a normal way, unless they actively involve themselves in aiding and abetting, would not have any liability. And I have never, certainly in the Library of Congress, I would never expect there to be liability because the library would never aid and abet, to my knowledge.

Ms. LOFGREN. Aiding and abetting is one of the issues that has been of concern. This is something that in the whole copyright arena, as we move into the Internet era, there is going to be a lot of thinking and readjusting. I mean not just in Congress, but in society and how we think about our existing laws and how they apply to this wonderful new world.

In your judgment, if one makes available a search engine or a browser or a hypertext link, is that aiding and abetting?

Ms. PETERS. That is an interesting question. I do not really have an answer. I have to go back and think about it. We have looked at linking in relation to our own site, what should we link to?

And we made a determination that we were going to be very close in what we link to because we wanted to limit any possible liability and we did not want anybody saying that we had linked to a pirated site.

I think that maybe the online service providers could answer how the links are made, and I think maybe you can answer that more.

Mr. DI GREGORY. I do not think that we are trying to do, nor does this law try to prevent the dissemination of information. What

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 27 1999

we are looking to try to prevent is people intentionally disseminating copyright information.

I do not think this statute requires anything of the service providers other than to—other than not engaging in intentionally providing copyrighted information.

Ms. LOFGREN. I think we are of one mind, really. I am just trying to explore unintended consequences here which is important to do in the Internet age.

Ms. PETERS. Clearly you would aid and abet if you had a site that said, "Top ten pirated sites," and led everybody to them.

Mr. DI GREGORY. I do not know that—yeah. I do not know that we would necessarily prosecute them because you have got to look at all the facts and circumstances before you make such a decision.

But I think certainly we are not looking at simply prosecuting somebody for passing on copyrighted information if they had no intention of passing on copyrighted information. And maybe there is a more articulate way to say it, but I cannot come up with it right now.

Ms. LOFGREN. Mr. Chairman, Mr. Delahunt just asked if I could yield for a follow-up. I do not have any more time. Perhaps you would let——

Mr. COBLE. It is going to be all right.

You may—without objection, the lady is asking for an additional minute.

Ms. LOFGREN. Mr. Delahunt, I will let you take my minute.

Mr. DELAHUNT. Mr. Di Gregory, I respect what you say about prosecutorial discretion. It seems to me that there is a legitimate concern about, prosecuting schools and librarians. I presume that it is not the position of the Department of Justice to initiate a special task force on copyright infringement to go around and focus in on the villages and towns of the United States, chasing librarians and similarly situated users.

Mr. DI GREGORY. We are aware of no need to do that. Right.

Mr. DELAHUNT. In fact, how many cases has the Division brought in this area other than the *LaMacchia* case?

Mr. DI GREGORY. I do not have an exact number.

Mr. DELAHUNT. Not a lot, though?

Mr. DI GREGORY. Not a lot.

Mr. DELAHUNT. OK. We're really talking about a situation, I presume, where there is a recognition that civil litigation has not been an effective deterrent in terms of the kind of scenarios that developed in *LaMacchia.*

Mr. DI GREGORY. That's right.

Mr. DELAHUNT. So now it has come to a situation where it is appropriate for Congress to determine and make a decision as to whether criminal sanctions will, in fact, deter.

Mr. DI GREGORY. That's right.

Mr. DELAHUNT. I think that's where we stand in terms of the policy.

I happen to have been a prosecutor in a former life, and I honestly believe that if there is such a concept as deterrence, this is one of those cases in which it can be effective. That is why, maybe with some tweaking and some amendments, I intend to support Representative Goodlatte's bill.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 28 1999

But I think the concerns that we have here, in many cases, are exaggerated. I really honestly believe that we are not going to see a rash of United States Attorney's offices sending out hordes of FBI investigators to track down librarians and teachers in schools. That is just not going to happen.

In fact, as was mentioned earlier, how do we even discover these crimes?

Well, the reality is, unless it is brought to you, you are not going to discover it. So it is going to be somebody who has a concern about his or her work being pirated who is going to complain to the United States Government.

Is that a fair statement?

Mr. DI GREGORY. I think in most cases, that is true.

Mr. DELAHUNT. Right. I mean these are not investigations that are initiated sua sponte?

Mr. DI GREGORY. In most cases, I think that is true.

Mr. DELAHUNT. Thank you.

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

The gentleman from Utah, Mr. Cannon. Recognize you for five minutes.

Mr. CANNON. Thank you, Mr. Chairman.

I am intrigued by the idea of the hyperlinks or the hot links. I think it would be following up on Mr. Delahunt's question.

I know in my district we have software producers who spend a great deal of time searching for people who are stealing their software through web sites.

It would seem to me that it is fair to say that if you have a hyperlink or a hot link that it would indicate some awareness, and therefore, would be an indicator to you, but not dispositive of willfulness, Mr. Di Gregory.

Mr. DI GREGORY. I think so. I mean that is certainly something that you would consider.

And I want to make the point again, just with respect to the determination of criminal intent, whether it is a violation of copyright or simply stealing an automobile, we are still talking about criminal intent to commit the act.

Mr. CANNON. Right. Now when you—in your opening statement, you pointed out you made your manual available on the Internet. I take it that is so people who are concerned about Internet theft of intellectual property will know what your standards are and how you proceed with those so they can help the accused for you?

Mr. DI GREGORY. Well, I—that—not necessarily know what our standards are, but become familiar with—hopefully help them become familiar with the copyright law and become familiar with the parameters within which we work.

Mr. CANNON. Thank you very much.

Mr. COBLE. Thanks, gentlemen.

The gentleman from Indiana, Mr. Pease, is recognized for five minutes.

Mr. PEASE. Thank you, Mr. Chairman.

Mr. Di Gregory, I wanted to go into the discussion you had with Mr. Goodlatte on the penalty section of the Bill, and I thought I heard you say that you would prefer a definition that did not go

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 29 1999

after the one-time offender or the person who occasionally violated—technically violated the copyright law.

Can you help me understand where you—what you said and where you were headed with that?

Mr. DI GREGORY. I think what we would like to do is work with the Committee on that because we want to make sure that the greatest deterrent effect possible occurs, and I think one of the ways you do that is to punish those persons who are trying to do more than just copy something for—for grandma, grandpa, brother or sister, and who were copying—as I think the Senate will suggest—ten or more copies with a certain value.

Mr. PEASE. The reason I ask is that I am the one who shares a concern with several members of the Committee on what has sometimes been called a tendency to Federalize crime.

But it appears to me this is an area where there clearly is a Federal crime. And so not to at least have a violation of that law, even a one-time violation be a criminal offense seems to me to be wrong. It should be a criminal offense.

And then we get into the question of prosecutorial discretion, about whether it ought to be prosecuted if there is a one-time violation.

Mr. DI GREGORY. Certainly, we do have exclusive responsibility in this area, but I think it is important also to keep in mind that there are civil remedies for even that one-time copy that can be pursued by the holder of the copyright.

And I think when you—when you consider whether or not you want to Federally criminalize that single copying event, even as a misdemeanor, you—and consider that we are it in that area, you also need to consider the resources that we have to devote to the enforcement——

Mr. PEASE. I understand that, but prosecutors do not prosecute every violation of the law.

Mr. DI GREGORY. Sure.

Mr. PEASE. They use their discretion, what resources are available. "How do we make a determination?"

It seems to me that we ought perhaps to look at a system of graduated penalties or something else that might reinforce the fact that you do not have enough resources, but not to say that any one violation ought not be a criminal offense, even if it is never prosecuted does not track for me.

Mr. DI GREGORY. As I said on other—we would certainly be willing to sit down with Committee staff and work that out.

Mr. PEASE. OK. I appreciate that.

Then related to that, the penalty provision that is included calls for three years of imprisonment.

Can you tell me how that compares with similar crimes, whether that penalty is in the same range of expectation for other electronic——

Mr. DI GREGORY. Or other kinds of theft?

Mr. PEASE. Yes.

Mr. DI GREGORY. I think it is within that range, but I would be glad to check on that for you with respect to the sentencing guidelines and the maximum penalties for those offenses and get back to you.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 30 1999

Mr. PEASE. OK. I appreciate it. Thank you.

Thank you, Mr. Chairman.

Mr. COBLE. I think the gentleman has a question.

Mr. DELAHUNT. No. As long as we do not make these mandatory sentences, Mr. Chairman.

Mr. COBLE. Ms. Peters, Mr. Di Gregory, we thank you for your testimony today and we will be in touch.

Ms. PETERS. Thank you.

Mr. DI GREGORY. Thank you, Mr. Chairman.

Mr. COBLE. The second panel will come forward, if you will. Mr. Robert Kruger is the Vice President of Enforcement of the Business Software Alliance, and Mr. Kruger, I will let you introduce your two witnesses who are with you, one of whom I think is amply represented in the Congress by the gentleman from California.

I will introduce, meanwhile, Ms. Sandy Sellers, while you all are preparing to be seated.

Sandy Sellers is the Vice President of Intellectual Property Education and Enforcement with the Software Publishers Association where she manages all intellectual property educational programs enforcement actions, both domestic and international.

Prior to joining SPA, Ms. Sellers was a partner in the Washington, D.C. office of William, Briggs, Hoffa, Gilson and Leone where, for ten years, she specialized intellectual property and litigation.

Prior to entering private practice, she was an attorney advisor to the Chief Administrative Law Judge of the United States International Trade Commission.

Ms. Sellers has served as President of the International Trade Commission Trial Lawyers Association and is active in the International Trademark Association.

She was awarded her Juris Doctor from George Washington University and a Bachelor's Degree from Dickinson College.

Now, Mr. Kruger, if you would like to introduce your witnesses.

Mr. KRUGER. Sure, Mr. Chairman. Thank you very much.

My name is Bob Kruger. I am Chief Enforcement Officer for the Business Software Alliance. Prior to joining BSA's fight against software piracy, I, too, was a Federal prosecutor fighting crime.

Mr. Chairman, I am not here to testify today. I think it is more important that the Committee hear directly from representatives of members of the Business Software Association who are, in fact, victims of software piracy. So I will allow them to speak to the Committee.

But I do want to say, Mr. Chairman, that I am available to the Committee, both now and at any time, to answer questions you may have and to share experiences that I have had on the front lines of this fight we are waging against software piracy.

I will say this: From my experience both as a prosecutor and representative of the industry, there is a critical need for effective law enforcement to deter this type of crime.

Greg Wrenn and Brad Smith are here, and I will let Brad lead off.

Mr. COBLE. Thank you, Mr. Kruger, and, folks, I will again remind you of the ever present red light. If you can comply with that, we will be appreciative.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 31 1999

It is good to have you all with us, so we will start with Mr. Smith and work from my left, or Mr. Wrenn, and then Mr. Smith, you want to follow him, and then Ms. Sellers?

STATEMENT OF GREG WRENN, SENIOR CORPORATE COUNSEL, ADOBE SOFTWARE

Mr. WRENN. Thank you, Mr. Chairman, Mr. Frank and members of the Committee. My name is Greg Wrenn. I am Senior Corporate Counsel with Adobe Systems. We are based in San Jose, California. Adobe was one of the leaders in providing desktop publishing technology. It was founded in 1982, and it continues to lead the market in providing tools for more imaginative and creative communication in print and electronic media, including the Internet.

I am pleased to testify today on behalf of the Business Software Alliance, with my colleague, Brad Smith, from Microsoft. We appreciate the time.

Let me begin first, Mr. Chairman, by thanking you for the opportunity to speak today, for the opportunity to have a hearing on this issue that is absolutely critical for the software industry.

We are grateful for your leadership, for the support of the Committee, and the opportunity to come today and address these issues. Mr. Frank, Mr. Cannon, we are grateful for your support of Mr. Goodlatte's introduction of H.R. 2265.

And while I am on the thank you's, I would also like to express my thanks to the Copyright Office and the Department of Justice for their support today on these issues and their ongoing support of some of the difficult industry issues that we face.

What I would like to do today is tell you a little bit about the software industry, describe a bit of the piracy problem that is eating away at the industry, and then briefly address some of the things that we think this Committee may be able to do to help address the problem.

The software industry is probably the greatest success story of American business. From 1980 to 1992, the software industry grew at an annual rate of 28 percent, compared with about a three percent rate for the domestic economy.

There really is no sector of the American economy that has not enjoyed the benefits of the information revolution that the software industry has brought about. The software industry directly employs about 620,000 people. That figure does not include upstream and downstream ripple effect on jobs and economic activity in other sectors by the software industry.

The software industry is, of course, a huge export business and America is fortunate in having American publishers control about 70 percent of the world market.

The software industry is also probably one of the best at investing in the future of this country. In 1995, nearly nine percent of all U.S. industry research and development investment was made by the members of the Business Software Alliance. That is not the software industry as a whole, that is just the few members of the Business Software Alliance. These details which are included with my testimony in a report that the BSA commissioned, by Nathan & Associates, has the statistics and the background information. It

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 32 1999

is very useful in showing the role of the software industry in the economy.

Let me turn now to the piracy problem. Piracy is probably the biggest threat to this economic engine. Mr. Chairman, you were right in first announcing these hearings, to say that piracy is just a fancy word for theft. And the fact of the matter is, the software industry is being robbed blind.

People know now, for the most part, that piracy is a problem around the world. The studies show a 43 percent rate of piracy worldwide. Roughly one in two copies of software in use is an illegal copy. A lot is heard about problems in China and other regions throughout the world.

The fact of the matter is, when you look at the statistics, our biggest piracy in the world is in the United States. We might have a relatively low piracy rate, although I hate to call it low, of 27 percent. That is, what, one in four copies in use of an illegal copy.

Although the rate might be lower than 94 and 97 percent piracy rates we see in some countries, the rate of piracy, times the size of the market, creates a loss greater in the United States than anywhere else—$2.3 billion in 1996.

This is not just a problem that affects the software industry. What this means for America overall is that in 1996, 130,000 jobs were lost due to piracy in this country. It meant a billion dollars in tax revenues to this country. This is a huge problem for all of us.

The piracy takes many forms. Our biggest problem is with what we call "end user copying," businesses that buy one copy and put it on ten machines, or consumers that buy a copy and share it with all of their close friends. That is the biggest loss for us.

Internet piracy is a huge problem and that is what we are here to address today. And if I may finish briefly. I realize the light is on, Mr. Chairman, but if I can just wrap it up.

Internet piracy is simply out of control. It is basically Dodge City out there. There is no law.

The Department of Justice and the FBI have been willing to help, but their hands are clearly tied by a lack of law enforcement tools, particularly by the loophole created by *LaMacchia* problem. Their hands are tied by the lack of jurisdiction to go around and address these cases. So it is critical that we have this addressed.

So, again, we want to thank you for holding this hearing. This is an incredibly important first step in addressing the piracy problem. This has been a great opportunity to address the piracy issues and H.R. 2265, and to recognize the support that we have seen in moving it forward.

And then what I would like to do at this point is turn to my colleague, Brad Smith from Microsoft, who will detail some more proposals, as well as Sandy Sellers from Software Publishers Association, and we look forward to an ongoing dialogue with this Committee and Congress.

Mr. COBLE. Thank you, Mr. Wrenn.

Mr. Smith.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 33 1999

STATEMENT OF BRAD SMITH, ASSOCIATE GENERAL COUNSEL, INTERNATIONAL LAW AND CORPORATE AFFAIRS, MICROSOFT CORPORATION

Mr. SMITH. Thank you, Mr. Chairman. My name is Brad Smith. I am the Associate General Counsel at Microsoft responsible for the company's International Law and Corporate Affairs including all of our anti-piracy and anti-counterfeiting work worldwide, I would like to second what Mr. Wrenn said in conveying our appreciation for the opportunity to address this issue today, and certainly for all of the leadership shown by the members of this Committee and by the Copyright Office and the Department of Justice.

As Mr. Wrenn said, Internet piracy is a real problem for the industry. It is not the biggest piracy problem today, but it is far and away the fastest growing problem. Indeed, Internet piracy is growing at such a fast rate that I find that one of the biggest challenges that we face in the industry is simply having to reeducate ourselves every six months about its most recent dimensions.

I thought it might be most useful to give you a sense of our chief concerns by providing having a brief demonstration of the way that we now find piracy on the Internet I believe there is a projector that will show a computer screen to the wall.

The first thing that we are going to do is user browser software to take you to two sites that are on the Internet. Both of these are screen shots that were downloaded from the Internet.

The first thing that, in fact, this demonstrates is the sometimes somewhat odd vocabulary that people who distribute piracy on the Internet use. I think we are going to end up having to publish an Internet piracy dictionary before we are done.

As you see on this site, the first reference is called, "Too Slow's Secret Warez." That word, "warez," w-a-r-e-z, is in fact, a slang term that refers to pirated software that is available for downloading. And, indeed, if you go to one of the text search engine index services that are now frequently available on the Internet and do a search for the word, "warez," you will find that there are now 17,000 pages on the Internet where that word appears. While you may not find software for downloading available on each and every one of those pages, there probably are more than 10,000 sites on the Internet today where you can download illegal software.

If we go to just one of these, the first one on this page, Radiation King, at the bottom, this is what you would find. This is the page that would appear on somebody's computer screen. Most of these folks do a nice creative job of their own logos, but what you really find is lots and lots of software. While the red letters here are a little hard to read, each of those lines is a reference to a software program available for downloading. You will find Microsoft programs such as Microsoft Plus, and a number of other programs. If you simply point to the program that you want with your mouse and click once, this site will download that software onto your computer. It is really as simple as that. Once you find the site, just scroll down the page, click on the program of your choice and it is yours.

We have really found a situation today where it is extraordinarily easy for people to download this software, and with the use of the search engines which are well known to many, many

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 34 1999

users of the Internet, it is extremely easy for people to find these sites.

There is another aspect that I wanted to demonstrate that is also characteristic. Unfortunately, the Internet piracy that is illustrated by this second site shows that what you typically find in a lot of these sites is, unfortunately, a lot more than copied software. A lot of people who get their thrills out of making this software available get their thrills out of other things, as well. This particular site, for example, also has what is called, "cracks." These are programs that will break copy protection on software so that more and more illegal copies can be made.

Another feature that this particular site offers is programs that enable someone to create what is called an e-bomb or an e-mail bomb. An e-bomb is, in fact, a device that allows a user of e-mail to, in effect, bombard someone else's e-mail address so that a person might receive say a thousand e-mails. And, indeed, when the Business Software Alliance takes action against somebody who is running this kind of site, it is not at all uncommon for them to receive an e-mail bomb that simply consists of a thousand e-mail messages, that, unfortunately typically consist of the repetitive use of four-letter words.

But it is just one example of the type of thing that these folks are engaged in.

That is all I have for the demonstration, so you can turn the lights back on.

Finally, these sites also are often run by people who get their excitement out of staying up until four in the morning and trying to crack their way into the Justice Department or somebody else's computer system.

They may not be making any money out of it. Typically, in this type of instance, they do not. But it is a real problem and we do need to take criminal action against it.

Thank you.

[The Statement of Brad Smith follows:]

PREPARED STATEMENT OF BRAD SMITH, ASSOCIATE GENERAL COUNSEL, INTERNATIONAL LAW AND CORPORATE AFFAIRS, MICROSOFT CORPORATION

Introduction

Mr. Chairman, members of the Subcommittee, my name is Brad Smith, and I am Associate General Counsel of International Law & Corporate Affairs at Microsoft Corporation at its headquarters in Redmond, Washington. Over the past twenty years, Microsoft has sought to empower personal computer users by developing software that makes it easier for them to use their PCs at home and at work for an increasing number of purposes. In pursuit of this goal, Microsoft has grown, changed, adapted and reinvented itself continuously—today we employ nearly 19,000 people, approximately 9,000 of which are located at our headquarters in Redmond, Washington. We are now one of the leading software publishers with products ranging from operating systems, to applications software such as word processing and spreadsheet programs, to software development tools and programming language products that help people develop and write creative software, and to an Internet on-line service, The Microsoft Network ("MSN").

I am pleased to testify today, along with my colleague Greg Wrenn of Adobe, on behalf of the Business Software Alliance (BSA).

The Business Software Alliance promotes the continued growth of the software industry through its international public policy, education and enforcement programs in 65 countries throughout North America, Europe, Asia and Latin America. BSA worldwide members include the leading publishers of software for personal computers: Adobe Systems Incorporated, Apple Computer, Inc., Autodesk, Inc., Bentley Sys-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 35 1999

tems, Inc., Lotus Development Corp., Microsoft Corp., Novell, Inc., Symantec Corporation, and SCO, Inc. BSA's Policy Council consists of these publishers and other leading computer technology companies including Compaq Computer Corporation, Digital Equipment Corp., IBM, Intel Corporation and Sybase.

I want to start by emphasizing what already has been said this morning—addressing the software piracy problem requires both better education and stronger enforcement of our laws. BSA has pursued such a comprehensive approach for many years. At BSA, we will be redoubling our education efforts—and we want to thank this Subcommittee for holding this hearing, which significantly helps in that regard. But we also believe we need to improve our enforcement tools and increase the laws' deterring effect.

Therefore, this afternoon, I would like to briefly review what we at BSA are doing to combat software piracy. Then I would like to turn to discussing the problem posed by software piracy via the Internet and the solutions presented in the NET Act, H.R. 2665.

BSA's Education and Enforcement Program

BSA's education efforts are designed to increase public awareness of the legal protection of software and encourage voluntary compliance with the copyright laws through responsible management practices. For example, for executives with responsibility for managing the purchase and use of software—including Directors for Purchasing, MIS professionals, Chief Financial Officers, Directors of Personnel, Internal Auditors, and Chief Executive Officers—the BSA offers the Software Management Kit, which includes information about establishing software management policies for all aspects of an organizational operation.

BSA experts speak at major computer trade shows, end-user meetings, government seminars, and association conferences—addressing critical issues, including software piracy as well as copyright protection and software licensing. Anti-piracy materials are regularly distributed, free of charge, to schools, user groups, government agencies and computer consultants.

But with respect to those who choose to violate our copyright laws, the BSA also undertakes enforcement actions against organizational end-users, resellers, Internet pirates, counterfeiters and other entities suspected of making, using or distributing illegal copies of software. These enforcement actions, which have included BSA provide the caller with software management materials or pursue the lead of suspected piracy to determine whether there exists sufficient evidence for an enforcement action against the alleged infringer.

Problem Of Piracy Via The Internet—The Need For H.R. 2665

Let me take just a minute to describe the situation posed by piracy via Internet Bulletin Boards or websites and the gap in the current laws illustrated by the *LaMacchia* case.

The Internet has made it virtually cost-free and risk-free for software pirates to reproduce and distribute copyrighted works on a commercial scale, displacing untold numbers of sales. In brief, an individual can set up a computer system such that others can gain access to valuable software programs through an electronic "bulletin board" and then download those programs onto their own computers free of charge. Often the individual may do this for commercial gain. But frequently individuals may steal software programs to demonstrate their technical prowess (i.e., to show they can do it), to build their personal collections by bartering with other pirates, or simply as a form of vandalism. Let me demonstrate for you how easy it is to pirate software on the Internet.

The problem we face is that if an individual steals thousands of dollars of creative works, posts them to a "bulletin board," offers to make such software freely available, and is prosecuted for these actions, the case will be dismissed—in large part because the Copyright Act states that software pirates are only criminally liable if they steal "for the purpose of commercial advantage or private financial gain." In *U.S.* v. *LaMacchia,* U.S. District Court Judge Richard Stearns noted that such activity was at best "heedlessly irresponsible, and at worst nihilistic, selfindulgent and lacking in any fundamental sense of values." But it was not, the judge found, a violation of the Copyright Act. However, the judge also stated that he believed "criminal, as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution." Clearly, then the law needs to be changed to cover such commercial-scale piracy.

For this reason, we are extremely pleased that Subcommittee Members Bob Goodlatte, Chairman Howard Coble,Barney Frank and Chris Cannon have intro-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 36 1999

duced H.R. 2265, the "No Electronic Theft (NET) Act." BSA strongly supports this legislation, and commends these Members for their leadership on this critical issue.

H.R. 2265 is vitally needed to ensure that copyright holders receive adequate protection in the digital environment. This bill makes it a felony under a new Section 17 U.S.C. §506 (a)(2) to willfully infringe a copyright by reproducing or distributing 10 or more copyrighted works, with a value of at least $5,000, within a 180-day period, regardless of whether the infringing individual realized any commercial advantage or private financial gain. The bill also adds a definition of "financial gain" in Section 17 U.S.C. § 101 to clarify that the term includes bartering for, and the trading of, pirated software. In other words, if you take a pirated software program and trade it on the Internet and eventually barter to the point where you have a $5,000 portfolio of software, the bill considers such bartering to be a criminal act—just as if you had sold the stolen software for $5,000.

In addition, H.R. 2265 ensures that victims of criminal copyright infringement will have the opportunity to provide victim impact statements to the court about the impact of the offense and directs the Sentencing Commission to ensure that guideline ranges are sufficiently stringent to deter criminal infringement of intellectual property rights, and provide for consideration of the retail value and quantity of the legitimate, infringed-upon items. Finally, the bill extends the statute of limitations for copyright infringement from 3 to 5 years.

I want to be very clear that we are *only* talking about *willful infringement* of a copyright holder's rights. H.R. 2665 merely strengthens criminal law against unscrupulous individuals. As this Committee well knows, under criminal law a willful act requires that it be intentionally done with knowledge that it was prohibited by law. H.R. 2265 does *not* address the potential liabilities of Internet Service Providers and other third parties that may innocently provide the means used by others for, but who themselves do not engage in, willful copyright infringement.

Moreover, we believe that because this is a criminal statute with criminal liability, the possibility of longer sentences should be focused on the more serious offenses. Thus, we believe for piracy of copyrighted works which have a total retail value of more than $10,000, imprisonment of up to three years would be in order. At the same time, we would like to suggest penalties for repeat copyright offenders be increased. In those instances where a fine is imposed in lieu of imprisonment, there should be a significant minimum fine with the possibility of up to double the otherwise applicable maximum possible fine.

We strongly support the provision extending the statute of limitations for copyright infringement from three to five years. Such a five-year statute of limitations is the norm for criminal violations under Title 18 of the United States Code.

We also support the provisions of the bill directing the Federal Sentencing Commission to comply with the statutory definition of "retail value" to ensure that applicable penalties are based on the retail value of the legitimate items being infringed. We also believe that the Commission should be required to consider restitution as an element of sentencing and that statutory damages should be awarded according to the nature of the offense and without regard to the infringers' ability to pay.

In addition to the important changes made by H.R. 2265, the Subcommittee also may wish to consider in the near future other amendments to the Copyright Act which could help further reduce piracy. For example, we believe the minimum statutory damages for piracy should be increased to have the desired deterrent effect on piracy. The Subcommittee also might consider the creation of tiers of damages, imposing higher levels for categories of willful piracy. Importantly, we believe that courts should be required to double the amount of damages (whether actual or statutory damages) for repeated piracy violations. Thus, where a recidivist commits piracy the court would be required to double the amount of damages. Finally, the Subcommittee might wish to review the procedures available to those seeking to enforce their intellectual property rights to ensure that they can obtain evidence to prove piracy.

Conclusion

Mr. Chairman, Members of the Subcommittee, we understand that an unfortunate but currently inescapable part of our job is to protect our intellectual property from those who simply would steal it. Certainly BSA members are doing what we can to educate users about the practical, business and legal consequences of using pirated software. But we also are committed to pursuing those who willfully choose to violate our intellectual property rights and pirate our products.

We sincerely hope that the Subcommittee moves forward with H.R. 2665 expeditiously. We believe it will prove to be of great significance in helping to crack down on software piracy.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 37 1999

Mr. COBLE. Ms. Sellers?

STATEMENT OF SANDRA A. SELLERS, SOFTWARE PUBLISHERS ASSOCIATION

Ms. SELLERS. Chairman Coble, Mr. Frank and other distinguished members of the Committee, I am Sandra Sellers, Vice President of Intellectual Property Education and Enforcement for the Software Publishers Association. I appreciate the opportunity to testify today and ask that my written testimony also be placed in the record.

The SPA represents over 1200 companies, including my co-panelists, Adobe and Microsoft. They develop, market and distribute software for the education, entertainment, business and Internet.

Our mission is to promote and protect the entire software industry and almost 900 of our members have authorized SPA to enforce their intellectual property rights.

SPA calls upon you today to do three things to help diminish software piracy.

Number one, lead by example by making the Federal Government accountable for using only licensed software, by implementing software asset management programs.

Number two, enact H.R. 2265, the No Electronic Theft Act, which would close the loophole and enable law enforcement to prosecute willful commercial scale Internet piracy, even in the absence of personal financial gain.

And, three, promptly enact H.R. 2281, the WIPO Copyright Treaty Implementation Act.

As Mr. Wrenn noted, in 1996, the industry lost over $11 billion worldwide. The most pervasive form of piracy contributing to these statistics, he referred to it as, "end user piracy." We sometimes call it, "softlifting," but that is the purchase of a license for software and loading it onto other unlicensed computers, thus exceeding the license. Softlifting can even be done by well-known, large corporations, and by government agencies.

Today I will relate two illustrations of why attention must be given to our government's software policies and procedures.

The purpose of this testimony, though, is not to accuse. Our purpose is to ask for accountability and to assist those agencies struggling to act responsibly.

In early 1993, the Department of Defense issued an audit report on controls over copyrighted computer software. The report sampled—did a sample audit of 1,022 computers out of the 377,000 computers then in use by the Department of Defense, and the sample audit found unauthorized software had been installed on 51 percent of the sample audit for a value of over $225,000 of pirated software.

The report concluded that the condition existed because controls to insure compliance with the license agreements and the copyright laws were either ineffective or nonexistent because management was indifferent to the problem.

The report, therefore, recommended that a guidance directive be issued. But despite several due dates over the past few years, that guidance directive still has not been completed and issued, and no follow-up reports have been done.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 38 1999

In July, 1996, SPA received a report that the Department of Labor's Mine, Safety and Health Administration, MSHA, was using illegal software at two of its locations.

DOL officials agreed to audit MSHA and to develop and implement software management and procedures for all of DOL. But the process has been extremely slow, largely due to bureaucratic red tape, and in my opinion, due to the need for all the Union review involved.

Though the DOL has been very cooperative, nearly 18 months will have passed between the time we first brought this to DOL's attention and the time the audit will have been completed. And during that time, if the status quo has been maintained, that may mean that illegal software is continuing to be used.

The reason? Lack of preexisting policy, lack of assignment of responsibility, and lack of procedures for follow through.

It may not be easy to implement these policies, but it is possible, and the SPA stands ready to help. We have available sample policies and guidelines, including a software management training seminar that has been taken by over 5500 people in 30 countries in the past three years, including government employees.

But neither industry nor well-meaning individual government employees can accomplish this task alone. SPA recommends a House resolution and an Executive Branch directive, that Federal agencies take the four steps that corporate America has taken, first step being to adopt a software management policy; two, assign responsibility for administering the policy; three, conduct regular audits to ensure compliance; and four, take corrective action, if needed.

SPA would be pleased to provide information and assistance in developing and implementing these policies.

I am pleased to report that the Administration has acted expeditiously. Two days ago while addressing SPA's 13th Annual Conference, Vice President Al Gore charged the Council of Chief Information Officers to develop uniform Federal policies for checking software and responding appropriately if illegal software is found.

He further directed them to work closely with SPA so that the Government adopts the very best commercial practices to send a loud and clear anti-piracy message at home and abroad.

Our Government must lead by example, both in the United States, and as an example to our foreign trading partners. And what we say here today, though, should not be misconstrued nor relied upon by foreign governments as an excuse for their own use of pirated software.

Our call for comprehensive, consistent management practices to promote accountability, and the Vice President's directive, reenforce our Government's commitment to respect copyright laws and to be held accountable under them.

We ask for your reenforcement by issuing House resolution.

Mr. Chairman, if I may make one or two brief remarks about H.R. 2265 and I will wrap up.

Mr. COBLE. Without objection.

Ms. SELLERS. The NET Act is essential to the fight against piracy on the Internet. We must close the LaMacchia loophole.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 39 1999

The people who created the waresites demonstrated by Mr. Smith often create them only for self-aggrandizement, and they are not deterred by a possible civil monetary judgment, because it probably would not be collectible against them. The threat of criminal prosecution is really the only effective deterrent against these kind of Internet pirates.

Now addressing Mr. Frank's question earlier about willfulness, I have no problem with adding something in the legislative history that would say the NET Act is not attempting to change the definition of "willfulness", or the willfulness standard. But I would put a period there. I would not then go on to include the different types of people who may or may not fall into it because the willfulness standard is a conduct-based activity, and if the conduct is appropriate, they will meet the willfulness standard. If they do not, they will not meet the standard.

We also agree with the Department of Justice's bill that the value threshold of $5,000 must include an aggregate, a choice——

Mr. COBLE. I am not sure—I am being very lenient with the witnesses——

Ms. SELLERS. I am sorry.

Mr. COBLE [continuing]. But wrap it up, if you can.

Ms. SELLERS. This is my last point.

The $5,000 threshold is very important because many of our publishers or entertainment and education publishers whose software retail for a value of $39 or $49, it is very important with a drop in software prices that the $5,000 threshold be kept at 5,000 and that it be an aggregate of either the software posted or the software downloaded.

Thank you very much, Mr. Chairman.

[The Statement of Ms. Sellers follows:]

PREPARED STATEMENT OF SANDRA A. SELLERS, SOFTWARE PUBLISHERS ASSOCIATION

SPA commends the subcommittee for holding hearings on these critical issues to the computer software industry. SPA is the leading trade association of the computer software industry, representing over 1200 companies that develop and market software for entertainment, business, education, and the Internet.

Our mission is to promote and protect the interests of the entire software industry. Electronic commerce in software promises to improve the odds of success for companies large and small, but its promise is threatened by the persistent and virulent problem of software piracy—the unauthorized copying and distribution of computer programs. In 1996, piracy cost the software industry over $2 billion in the U.S. and over $11 billion around the world. Year after year, software piracy remains a leading concern for hundreds of CEOs, one of whom recently called piracy "the single worst problem now facing the industry."

SPA believes that copyright should protect software on the Internet no less than software in CD–ROMs and other media. Virtually all software companies rely on copyright to protect their software, and hundreds look to SPA to help them protect their copyrights. For over a decade, SPA has fought software piracy through three lines of defense—education, enforcement, and advocacy for adequate laws to protect valuable copyrights and maintain the incentive to create—and is now active in about 20 countries. Moreover, one year ago we launched our Internet Anti-Piracy Campaign, and have learned valuable—and frightening—lessons about the changing tactics of software pirates.

New forms of software piracy are taking advantage of loopholes in current law. Under current law, showing financial gain is required to prove criminal (but not civil) copyright infringement. Because much software piracy on the Internet apparently occurs without the exchange of money, the so-called "LaMacchia Loophole" discourages law enforcement from taking action against willful, commercial-scale software pirates who eschew cash in favor of notoriety or bartering in "hot" software. One federal court speculated that such piracy could not be prosecuted for criminal

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 40 1999

copyright infringement, even though the defendant was alleged to have bartered for more than $1 million in stolen software. Moreover, it is not clear that current copyright law can reliably stop pirates from unauthorized circumvention of technical protection—an important supplement to legal protection—that controls access or copying of computer software. Many Internet sites already offer unauthorized passwords, serial numbers, and cracker/hacker utilities that permit Internet users to copy pirate software—the equivalent of stealing breaking into a bookstore to steal a book. Finally, SPA's independent investigation indicates that some federal agencies themselves have fallen short of what we have asked corporate America and other governments to do—be accountable for using only authorized software in their operations.

The clear message is that the U.S. government and governments everywhere must do more to combat software piracy at home, around the world, and on the Internet. SPA calls on Congress to take the following steps: (1) promptly implement the WIPO Copyright Treaty by enacting the WIPO Copyright Treaty Implementation Act (H.R. 2281), (2) close the "LaMacchia Loophole" by enacting the No Electronic Theft (NET) Act (H.R. 2265), and (3) lead by example by making Congress and the federal government accountable for using only licensed software by implementing a software asset management program. SPA hopes that this subcommittee and Congress as a whole will take these steps and join the fight against software piracy.

CURRICULUM VITAE OF WITNESS

Sandra A. Sellers is the vice president of intellectual property education and enforcement for the Software Publishers Association (SPA), where she manages all intellectual property educational programs enforcement actions, both domestic and international.

Prior to joining SPA, Sellers was a partner in the Washington, D.C., office of Willian, Brinks, Hofer, Gilson & Lione, where for 10 years she specialized in intellectual property litigation. Before entering private practice, Sellers was an attorney-adviser to the chief administrative law judge of the U.S. International Trade Commission.

Sellers has served as president of the International Trade Commission Trial Lawyers Association and is active in the International Trademark Association. She received her Juris Doctor from George Washington University and a bachelor's degree from Dickinson College.

DISCLOSURE OF FEDERAL GRANT, CONTRACT OR SUBCONTRACT RECEIVED

In the current and preceding two fiscal years, the Software Publishers Association has received the following federal grants, contracts, or subcontracts:

Department of Commerce, International Trade Administration, Award No. 95–3141 Oct. 1. 1995—Dec. 31. 1996 (as extended). SPA received $53,489 to present CSM software asset management training throughout Latin America.

Department of Commerce, International Trade Administration, Award No. 94–3185 Oct. 1, 1994 through Sept. 30, 1998 (as extended). SPA and its joint venture partners—the American Electronics Association and the Telecommunications Industry Association—received $440,000 (as amended) in matching funds to establish and operate the U.S. Information Technology Office, a trade development organization based in Beijing.

The witness has not personally received any federal grant, contract, or subscontract in the current and preceding two fiscal years.

Mr. Chairman and Members of the Subcommittee: I am Sandra Sellers, vice president of intellectual property education and enforcement for the Software Publishers Association (SPA). For over three years, I have been responsible for SPA's worldwide programs to protect computer software from piracy—programs that balance education with legal enforcement.

SPA commends you for holding these hearings on a grave and chronic problem facing the software industry—piracy at home, abroad, and on the Internet. We commend you and your co-sponsors for introducing the WIPO Copyright Treaty Implementation Act and Rep. Goodlatte for introducing the NET Act, two measures that would close loopholes now used by software pirates.

SPA is the leading trade association of the computer software industry, representing over 1,200 companies that develop and market software for entertainment, business, education, and the Internet. Our mission is to promote and protect the interests of the entire software industry, and year after year software piracy remains a leading concern for hundreds of CEOs and senior executives. As a result, hundreds

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 41 1999

of software companies look to SPA to protect and enforce the intellectual property in their software.

The Threat of Software Piracy

Software piracy, quite simply defined, is the unauthorized use of computer software. Software piracy occurs in several forms: (1) *softlifting,* which is purchasing a license for software and loading it onto additional computers, thus exceeding the license. This includes sharing commercial copyrighted software with friends, co-workers and others; (2) *counterfeiting,* which is the illegal duplication and sale of copyrighted software; (3) *hard disk loading,* whereby computer hardware dealers load unauthorized copies of software onto the computer's hard disk, often as an incentive for the end user to buy the hardware from that dealer; (4) *renting* software for temporary use without authorization; and (5) *uploading and/or downloading* copyrighted software without authorization via modem to or from the Internet or electronic bulletin boards. This testimony will focus on two of these types, softlifting, particularly by government entities, and Internet piracy.

The most pervasive form of piracy continues to be softlifting of entire computer programs, usually of business application software, for business purposes. In an independent study done earlier this year, we found that in 1996 piracy of business applications cost the industry over $11 billion worldwide, and over $2 billion in the United States alone. Forty-three percent of software in use worldwide is pirated, and in the United States 27 percent is pirated. These are conservative numbers for many reasons, chiefly because they include only business application software, and do not begin to count the revenue lost to the education, entertainment and other sectors of the U.S. software industry. Additionally, these numbers do not account for illegal copies distributed via the Internet, since it is impossible to track the amount of downloads of pirated software.

According to a recent Price Waterhouse survey, CEOs of software companies rank software piracy in the top 10 of their concerns. As Garry McDaniels, chairman of Baltimore-based SkillsBank Corporation, a leading educational software company, said, "To keep up with consumer demand and our competitors, Skills Bank has spent an average of 25 percent of our revenues in research and development. That investment could be seriously undermined by losses from software piracy."

For Todd Hollenshead, CEO of Texas-based id Software, Inc., which developed the best-selling games "Quake" and "Doom," the future of entertainment software online is threatened by piracy. "We believe that half of the full versions of "Quake" being played are pirate copies," said Hollenshead. "Software piracy is the single worst problem now facing the industry."

Indeed, the potential for replicating id Software's experience is frighteningly real because of the large number of pirate sites and the extensive listings of software titles available for free (but unauthorized) download. Anyone using any popular search engine can find "warez," the Internet term for pirate software. More experienced Internet users can access "elite" site on the Internet Relay Chat (IRC) or file transfer protocol (FTP) sites.

Imagine any other industry in which almost 50 percent—or even 27 percent—of goods produced were stolen; certainly that industry would not survive for long. It is imperative that everything possible be done to stem the tide of software piracy in the United States.

Who are the software pirates? There are even more types of software pirates than there are types of software piracy. The *"softlifters"* are often ordinary persons who may not realize they are breaking the law—they may believe that because their employer bought some software licenses, that it is okay to load those licensed copies onto other, unlicensed machines. Or maybe the "softlifters" do know that they are exceeding the license agreement and breaking the law, but believe they are "in the right" to save their employer money. We often hear this excuse from small businesses and educational institutions. "Softlifters" can include large corporations, small businesses, educational institutions, and even government agencies, state and federal. Regardless of who or why, these pirates cause great commercial harm to software companies.

The Internet has given rise to another type of pirate, the consummate "hacker" or "warez" aficionado, who copies and distributes computer software simply for self-aggrandizement—the reputation, the thrill, the "fun" of having the latest programs or the biggest "library" of "warez" titles. Take Max Butler, the courier for an Internet gang who hacked into servers operated by ABWAM, a Colorado-based Internet access provider, and created an FTP site crammed with dozens of pirated software titles. It is impossible to know how many illegal copies were downloaded from Butler's site before ABWAM, during routine server maintenance, found the telltale signs of Internet piracy—exceedingly large file transfers, a large number of

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 42 1999

uploads, and filenames representing commercial software titles. ABWAM reported the matter to SPA, which brought a lawsuit against Butler. With the help of Internet Service Providers, SPA has been able to identify other of pirate site operators. SPA has entered into several setlements with Internet pirate site operators, the terms of which included injunctions and community service.

Next week, SPA will commence a civil action for copyright infringment Fairest another Internet pirate. This suit will allege the posting of hundreds and hundreds of serial numbers and cracker/hacker utilities on the Internet. The sole purpose of these utilities is to bypass copy protection imbedded in commercial software. The availability of these utilities makes any commercial software program available in full form, for free, on the Internet.

For software companies, the Internet promises to be an alternative computing platform, which will need computer software to operate. It also promises to be a low-cost method for distributing software. Electronic commerce in software promises to improve the odds of success for companies large and small. It will free them from shrinking retail shelves and help keep the barriers to entry low enough for start-up companies. It will fulfill these promises only if is not threatened by the persistent and virulent problem of software piracy.

The Ongoing Fight Against Software Piracy

In its mission to promote and protect the interests of the entire software industry, SPA has fought software piracy through education, enforcement, and public policy. The first line of attack against software piracy must always be to ensure that adequate laws exist to protect this valuable intellectual property and continue to provide the incentive to create new products.

Along with appropriate laws, SPA advocates extensive public education about those laws, license agreements, and how to use software legally. SPA distributes a wide variety of educational materials, from free pamphlets to videotapes and extensive manuals of software asset management. SPA even teaches two fullday seminars: the Certified Software Manager (CSM) course in software management, which has been taken by over 5,500 persons in 30 countries in the last three years; and the Internet in the Workplace course, which guides organizations through the job of setting up policies for Internet usage by employees.

The third line of defense against software piracy is enforcement. SPA has actively enforced it's members copyrights in the United States for many years through lawsuits, cooperative audits and cease and desist letters. It now has enforcement programs in approximately 20 key countries worldwide. But enforcement can only be as good as the law upon which the efforts are based. There are actions that Congress needs to take now to fill certain voids.

Copyright Law—The Bulwark Against Piracy

To fight piracy, software companies need adequate and effective laws to provide legal protection for their works. Copyright law in the United States and other countries protects computer programs from unauthorized duplication, distribution and certain other uses. That is why virtually all software companies rely on copyright to protect their software from piracy, and why SPA believes that copyright should protect software on the Internet no less than software in CD–ROMs and other media.

In this way, copyright law provides software companies with the incentive to create new generations of software, and the confidence to experiment with new, more flexible means of exercising their rights. Nonetheless, changes are needed to close some loopholes that software pirates are using to upset the balance even more.

Closing the "LaMacchia Loophole" for Software Thieves

Much software piracy on the Internet uncovered by SPA apparently occurs without the exchange of money, even though it threatens large-scale harm to software companies. Under current law, showing such financial gain currently is required to prove criminal (but not civil) copyright infringement. In the 1994 court decision *United States* v. *LaMacchia* a federal court in Massachusetts dismissed wire fraud charges against a college student. The Court, in *dicta* further speculated that the defendant, an operator of a computer bulletin board who allegedly distributed more than $1 million in pirated software, also could not be prosecuted for criminal copyright infringement because he had received no payment for the pirate software.

The fact that willful, commercial-scale software pirates eschew cash in favor of barter or notoriety should not prevent law enforcement from prosecuting them for criminal copyright infringement. If one were to walk into a jewelry store, steal some jewels, and then give them away on the street to passersby without taking compensation for the stolen jewels, the thief would probably be prosecuted, despite the

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 43 1999

fact that he did not gain financially from his actions. The same should be true with respect to software.

SPA, therefore, strongly supports the "No Electronic Theft Act," H.R. 2265, introduced in July by Rep. Goodlatte and co-sponsored by Reps. Coble, Cannon and Frank. This bill would remove the financial gain requirement and make willful software piracy a crime if done for barter or causes at least $5000 in harm.

Technical Protection—An Important Supplement to Copyright Law

Another loophole is circumvention of technical protection to control unauthorized access or copying of computer software. Such technical protection promises to be an important supplement to the legal protection of copyright. Many software companies already rely on serial numbers and passwords to control installation of pirate software. Others rely on hardware copy protection (called "dangles"). Other copy control mechanisms to prevent unauthorized copying are available. Yet Internet sites which offer unauthorized serial numbers and cracker/hacker utilities which circumvent other copy protections are proliferating. Some Internet sites offer pages and pages of single-spaced material listing serial numbers which permit one to access otherwise inaccessible copies of commercial copyrighted computer programs. The same sites often also post many pages of hacker/cracker computer programs which can circumvent copy protection measures embedded by the copyright owner.

Persons who create and distribute these circumvention devices also have attempted to extort money from our members. Last year, someone attempted to extort $1 million from Symantec Corp. The blackmailer threatened to post on the Internet a circumvention program for one of Symantec's copy-protected programs. Such would have compounded the piracy of the program.

California-based SciTech Software, Inc. has a product called "Display Doctor." As part of the marketing for Display Doctor, Sci-Tech offers 21-day trial versions. Last May, Sci-Tech received demands from an online extortionist threatening to make available on the Internet the means to circumvent the timer software controlling the 21-day evaluation period. The online blackmailer demanded payment of $20,000. According to Kendall Bennett, Sci-Tech's engineering director, "The scary thing is not that our protection could be circumvented—dedicated pirates can always do that. What's scary is that they can get the information on how to circumvent into the hands of millions of casual users who would normally license our software."

The immediate threats to SciTech and Symantec have passed, but the blackmailers are Dill lurking. Unfortunately, it is not clear that current copyright law can be used to stop this kind of unauthorized circumvention, even though the purpose is software piracy. That loophole would be closed by the new WIPO Copyright Treaty, which requires the United States and other countries to make sure that software companies have effective remedies against circumvention of technical protection for copyrighted works. SPA has spent months building consensus among industry and government on how to do so, and Congress is now considering legislation.

Another Role for Government—Leading by Example in the Fight Against Softlifting

For nearly three years, SPA has used its "Benchmarks for Intellectual Property Protection" to assess whether U.S. trading partners are meeting their obligations to protect and enforce intellectual property rights in computer software. An important benchmark is a demonstrated commitment by national governments to the protection and enforcement of intellectual property rights in computer software. One essential way to demonstrate this commitment is for federal and state governments to cease using illegally copied software.

The U.S. government has been a vigorous advocate for this position in negotiations with our trading partners. For example, the 1995 U.S.-China IPR Agreement commited China to using only legal software in its government operations. Now, we issue a challenge to the U.S. government to again demonstrate its leadership by providing the administrative follow-through necessary to do what SPA has long asked of corporate America implement a comprehensive and verifiable software asset management program.

Some congressional offices and federal agencies have already undertaken this challenge, but it has not been undertaken by the federal government as a whole. Rep. Sonny Bono (R-Calif.) has long been interested in taking steps to ensure that congressional offices use software responsibly, and we applaud and support his efforts. But there has never been a directive from the President or Congress that requires all federal government installations to have a comprehensive software management policy and to implement procedures to ensure that the policy is being followed. As our experience with certain government agencies has shown, such a directive from the top of the various branches of government is necessary to ensure that the federal government will abide by the copyright laws and to assist those agencies

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 44 1999

struggling to act responsibly. Two examples will demonstrate why such a directive is essential. A report attached to my testimony provides further detail of these instances.

In early 1993, the Department of Defense (DOD) issued an audit report on controls over copyrighted computer software. The report found that at the end of 1991, DOD had approximately 377,500 computers. The DOD Inspector General's Office conducted an audit of a sample 1,022 computers at 22 locations and found that unauthorized software had been installed on 51 percent. The report concluded that the condition existed because controls to ensure compliance with computer software license agreements and copyright laws were either ineffective or nonexistent because management was indifferent to the problem. The draft report recommended that the Assistant Secretary of Defense for Command, Control, Communications and Intelligence display leadership on the issue of compliance with federal copyright law by issuing a directive on the subject. SPA has vigilantly followed up on the recommendations in the DOD report. In June 1994, the Inspector General's Office informed SPA that a formal directive would be issued in July 1994, which was later postponed until January 1995, then to December 1995. As of mid-August 1997, the Inspector General's Office indicated that the guidance directive still has not been completed and that there have been no follow-up reports. Despite knowledge of illegal use of unauthorized software, it appears to SPA that DOD has not issued a directive, nor followed up to institute appropriate procedures and educate its workforce in the proper management of commercially available computer software.

In July 1996, SPA received a report that the Department of Labor (DOL)'s Mine Safety and Health Administration (MSHA) was using illegal software at two of its facilities. SPA sent MSHA an audit letter on Aug. 9, 1996. On Jan. 10, 1997, SPA met with DOL officials, who agreed to audit MSHA and to develop and implement software management procedures and policies for the entire Labor Department. DOL has worked diligently toward developing new policies and a plan for software management, but the process has been extremely slow. As a result of the need to promulgate a software policy and then complete the necessary steps to implement the new policy, nearly 18 months will have passed from the time SPA notified MSHA until the audit has been completed. During that time, we assume that the status quo has been maintained, which may mean that illegal software continues to be used. It is SPA's opinion that an executive directive or congressional resolution would have assisted this situation and perhaps given support to well-meaning government employees who are attempting to comply with the copyright laws. If policies and procedures had been in place, DOL easily could have produced copies of its policy, the report of most recent audit conducted, and the corresponding proof of licenses all in response to SPA's first letter.

As part of a project to monitor compliance by government agencies with software license agreements, SPA has contacted several others seeking copies of policies and audit reports. That project is ongoing.

It may not be easy to come into compliance, but it is possible and SPA stands ready to help. SPA has available sample policies and guidelines, including a training seminar in software management.

A government success story can be found in the state of Ohio. SPA received a report of illegal software use by the Ohio Lottery Commission and initiated an audit. As an outgrowth, SPA worked with state officials to design and implement a software management policy and procedures for the entire state of Ohio. As a result, the whole state government now has a verifiable process by which to ensure that Ohio state agencies are in compliance with U.S. copyright laws.

SPA therefore recommends that strong directives be issued from the highest government leadership to implement a software use policy in order to ensure government compliance with federal copyright laws. The U.S. government must declare itself a "piracy free zone" for computer software, thereby setting an example for the rest of the world.

Action Plan to Fight Piracy

The SPA "1997 Global Software Piracy Report," which is also appended to my testimony, concludes that software piracy impedes the continued growth of the software industry and its associated benefits. The clear message is that the U.S. government and governments everywhere must do more to combat software piracy at home, around the world and on the Internet. SPA calls on Congress to take the following steps:

> Promptly implement the WIPO Copyright Treaty by enacting the WIPO Copyright Treaty Implementation Act (H.R. 2281), which would provide effective legal remedies to prevent unauthorized circumvention of technical protection for computer software and other copyrighted works.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 45 1999

Close the "LaMacchia Loophole" by enacting the No Electronic Theft (NET) Act (H.R. 2265), which would enable law enforcement to prosecute willful commercial-scale Internet pirates for criminal copyright infringement, even in the absences of commercial gain; and

Lead by example by making Congress and the federal government accountable for using only licensed software by implementing a software asset management program.

SPA recommends a House resolution and an Executive Branch directive mandating that congressional offices and federal agencies take the same four steps that corporate America has taken: (1) adopt a software asset management policy that prohibits the use of unauthorized software; (2) assign responsibility and authority for administering this policy; (3) conduct regular audits to ensure compliance; and (4) take corrective action, if needed. SPA will be pleased to provide information and training to help the agencies develop, implement and administer such a policy.

Conclusion

SPA is determined to work with the U.S. government to ensure its leadership in fighting software piracy, both around the world and on the Internet, and to ensure that piracy does not impede the rapid development of reliable electronic commerce in digital products.

APPENDIX

Tab 1: SPA Preliminary Report on Federal Agency Compliance with U.S. Copyright Law and Computer Sofware Use

Tab 2: Audit Report, Office of the Inspector General, Department of Defense, Controls over Copyrighted Computer Software, February 19, 1993

Tab 3: Correspondence between SPA and Department of Defense, June 20, 1994–July 31, 1995

Tab 4: Correspondence between SPA and Department of Labor, August 9, 1996–May 27, 1997

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 46 1999

TAB 1

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 47 1999



SOFTWARE PUBLISHERS ASSOCIATION
PRELIMINARY REPORT ON FEDERAL AGENCY
COMPLIANCE WITH U.S. COPYRIGHT LAW AND
COMPUTER SOFTWARE USE

The United States Government is the largest employer in the country, and the largest user of information technology. It is by far, the largest purchaser of personal computer software in the world. Because of its size, geographical distribution and organizational complexity, the federal government is probably in a more difficult position than corporate America when it comes to managing and controlling the use of software by its employees. This size and bureaucratic nature make it more difficult for owners of intellectual property rights to monitor the use of software products by federal customers. Regardless whether it is more difficult to police unauthorized software use by government agencies, such is no justification for allowing it.

At a time when the United States is making the protection of intellectual property the cornerstone of its international trade policy, it is especially important that it take steps to make sure that its own house is in order when it comes to software use by its agencies. U.S. trade negotiators must be able to point to its own government as a model for intellectual property compliance to buttress demands that other countries pass and enforce state of the art intellectual property laws. For this reason, the United States government must take a top down approach to the management of its software assets.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 48 1999

As the following report shows, federal agencies have progress to make in their efforts to ensure that its employees are using software that has been legally acquired. Indeed, only when stringent policies are institutionalized and regularized by the federal workforce can the United States be certain that its agencies are in full compliance with U.S. intellectual property laws.

Software Publishers Association has been aware for years that federal agencies have difficulty controlling the illegal use of software in their offices. In two specific instances, SPA has confronted agencies with evidence of improper software use. However, SPA has been unable to make sure that such improper use ceased or that such agencies have instituted policies that prohibit the use of unlawfully copied software. With regard to other agencies, SPA's preliminary investigation suggests that many have no written, consistent policy governing employee use of software. With regard to those other agencies, SPA's investigation is continuing.

1. Department of Defense.

In February 1993, the Office of the Inspector General of the Department of Defense issued an audit report (No. 93-056) on Controls Over Copyrighted Computer Software. (App. Ex. 1). This report found that at the end of fiscal year 1991, the Department of Defense "hereinafter "DoD") had approximately 377,500 computers which it assumed were microcomputers. The DoD did not maintain an overall inventory of computer software and no reliable estimates were available indicating the cost to purchase software for microcomputers within the DoD. The report found it reasonable to assume that millions of commercially developed software programs were installed on DoD microcomputers.

The DoD report recognized that software vendors attempted to control the use of their products through license agreements that invoked the protections against copying found in the federal copyright act. The report also recognized that the DoD was bound by restrictions on software use found in

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 49 1999

the license agreements that accompanied software products in use on DoD computers.

The DoD Inspector General's office, as part of its audit, conducted a physical examination of a sample of 1,022 computers at 22 locations within the military departments. The audit found unauthorized software had been installed on 51 percent of the 1,022 computers it tested. The report concluded that the condition existed because controls to ensure compliance with computer software licensing agreements and copyright laws were either ineffective or nonexistent and because of management indifference.

The audit showed that unauthorized software had been installed on computers at each of the 22 military department activities audited. Unauthorized software remained on the computers despite the fact that prior notice of the purpose and the date of the audit had been given. The report noted that each activity had ample opportunity to remove unauthorized software from their computers; some commands had directed such removal. The report estimated that the value of the 1,381 copies of unauthorized or undocumented software found on the computers it inspected was about $227,000.

The report contained summaries of reports prepared by the Army and Air Force audit agencies. The Army audit agency conducted three multilocation audits from 1988 through 1990, covering the acquisition, use, control, and accountability of commercial software. The Army audit agency concluded that policies and procedures had not established to prevent, detect, or control unauthorized copying of commercial software. Based on a statistical sample, the Army audit agency found that 41 percent of the Army-owned personal computers had undocumented software valued at $21 million.

The Air Force audit agency issued 33 reports from 1987 through 1991 on small computer software management and 4 follow-up reports. The reports included reviews of three major command headquarters and 30 bases or activities. Unauthorized copyrighted software was found on computers in 28

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 50 1999

of the 33 reports. The Air Force audit agency recommended that unauthorized software be removed from Government owned computers. Only one of the follow-up reports stated that deficiencies had been corrected. In the other three follow-up reports, procedures had not been fully implemented to remove unauthorized software from computers.

The Inspector General's auditors were given various reasons why undocumented software was installed on the computers tested. The Inspector General found that the problem stemmed from ineffective or nonexistent controls and a lack of management emphasis on compliance with licensing agreements. The computer security officers who were interviewed during the audit reported that efforts to control copyrighted computer software were hampered by a lack of command emphasis on the importance of complying with copyright laws and licensing agreements.

In one instance, auditors tested 12 of 20 computers of a section of an Air Force squadron and found 21 unauthorized software programs. The squadron commander, when interviewed by the auditors, stated that he knew that unauthorized copies of software in excess of the quantities purchased had been installed on the squadron computers. He stated that due to insufficient funds, the required number of copies of the software could not be purchased, but that the software programs were needed for the squadron's mission and the mission came first.

The audit report concluded that the results were sufficient to show that licensing agreements for copyrighted software were ignored at all levels of command for each military department. When coupled with the reports of the Army and Air Force audit agencies, the report found compelling evidence that abuse of software licensing agreements had been and remained commonplace throughout the DoD:

> Most significantly, the audit showed that leaders and managers have not only acquiesced in the continuing abuse of software licensing agreements, but that they have directed actions that required violation of Federal copyright statute. Disregard of Federal law under the guise of expediency signals an

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 51 1999

> unacceptable breakdown in integrity and ethical behavior among those who are responsible.

The audit report found that formal controls over copyrighted computer software and formal procedures for implementing the requisite controls were necessary to ensure that leaders, managers, and computer users know and apply needed safeguards to preclude copyright infringement. With rare exceptions, the audit report concluded, existing guidance was generally ignored by the activities being audited.

The draft report recommended that the Assistant Secretary of Defense for Command, Control, Communications and Intelligence display leadership in the issue of DoD compliance with federal copyright law by issuing a directive on the subject. The recommendation that a "directive" be issued was changed in the final report to recommend that further "guidance" be issued.

Management was given an opportunity to comment on both the findings and the recommendation contained in the report. The Navy and the Air Force gave no comments. The Army concurred in both the findings and in the recommendation. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence concurred in the findings but disputed the recommendations. The Assistant Secretary of Defense contended that existing laws and regulations were already in place. The Inspector General persisted that:

> In view of the pervasion of the condition disclosed by the audit and for the specific reasons provided in the Audit Response section in Part II of the report, we request that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) reconsider the need for corrective action in this matter and provide additional comments in response to this final report.

SPA has been vigilant in following up on the recommendations set forth in the audit report. In June 1994, SPA sent a letter asking for an update on the status of the Inspector General's recommendations. The Inspector

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 52 1999

General's Office promptly replied that preliminary guidance in the form of a memorandum had been issued and that a formal directive was due to be issued by the Office of the Assistant Secretary of Defense in July 1994.

In August 1994, SPA again wrote asking for a copy of the directive that was to have been issued in July 1994. The Inspector General's office replied, again promptly, that the directive had been delayed and was being readied for release in January 1995.

In May 1995, SPA wrote to the DoD FOIA office asking for a copy of the directive on computer software management. The Office of the Assistant to the Secretary of Defense for Public Affairs responded in July 1995 that the release date for the directive had been pushed to December 1995.

In August 1997, SPA contacted the office of the Director for Audit Follow-up at the DoD Office of the Inspector General. The information SPA was given indicated that the guidance directive that should have been issued in 1995 had not been completed as yet and that there have been no follow-up reports.

It has been over four years since the Inspector General of the Department of Defense issued his Audit Report finding that unauthorized software use by DoD employees was "rampant" throughout the department and recommending that the Assistant Secretary of Defense take a leadership role by issuing stronger and more explicit guidance on compliance with computer software licensing agreements. In the meantime, SPA has chronicled one delay after another in the issuance of that guidance. It appears to the SPA that the DoD has not issued any directive nor followed-up by instituting procedures and educating its workforce in the proper management of commercially available computer software assets.

2. Department of Labor:

In July 1996, SPA received a report that unauthorized computer software was in use at the Lakewood, Colo. and Arlington, Via. sites of the

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 53 1999

Department of Labor's Mine Safety and Health Administration (MSHA). The report indicated that 40 percent of the software in use on both servers and stand-alone machines was unauthorized. On Aug. 9, 1996, SPA sent a standard letter requesting permission to audit the MSHA computers in Lakewood, Colo.

SPA subsequently received a letter dated Aug. 13, 1996, from MSHA in Colorado challenging the veracity of the report received by SPA. The letter also denied SPA's request for permission to conduct an audit of the MSHA's computers. The letter suggested that, with respect to computer software, the MSHA was in a different position than a private company or organization because it was a government agency of the United States Department of Labor.

SPA responded to the letter with a letter dated Aug. 19, 1996, that named the specific software titles that were being used by MSHA employees without authorization, and suggested that a cooperative audit be conducted.

By letter dated Sept. 18, 1996, MSHA responded that, after discussing the matter with counsel, there could be no agreement that an audit could be conducted or to bind the agency to pay monetary penalties. The response also claimed that any efforts expended towards ensuring the MSHA computers contained only authorized software would result in an enormous, unreasonable, and unjustifiable drain on agency resources, and would interfere with the agency's primary mission. In addition, the response claimed that the magnitude of the alleged problem was insufficient to warrant the investment of time and resources. The response did state that a re-examination of the agency's policies and practices would be undertaken and that a management plan would be developed.

SPA responded on Dec. 10, 1996, with an insistence that federal agencies were equally subject to the copyright laws and persisted with a request that a cooperative audit be conducted.

Officials of the SPA and the Department of Labor met on Jan. 10, 1997. At that time, Department of Labor officials agreed to a software audit of

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 54 1999

MSHA over a 10 month time period and that the Department of Labor would develop and implement procedures and policies to heighten awareness and maintain compliance.

On Feb. 5, 1997, SPA received a letter from the Department of Labor forwarding a draft software usage policy. The letter, however, explained that the Department of Labor could not implement any new policy unless and until it have been reviewed and approved by the Department's two labor unions.

By letter dated May 27, 1997, Department of Labor notified SPA that it had developed a plan for enhancing software management within MSHA. The letter also indicated that a new position of software coordinator had been created which would be filled by July 1, 1997. However, the letter stated that the audits of the Lakewood, Colo. and Arlington, Va. MSHA sites could not be completed until Dec. 30, 1997, nearly 18 months from the time SPA first notified MSHA that there was a problem with unauthorized software use.

3. Other Agencies:

Beginning in July 1997, SPA commenced an investigation, using the Freedom of Information Act, of several other government agencies to determine whether they had in place comprehensive policies for the management and control of the use of computer software and procedures to ensure that their computers did not contain any unauthorized computer software. At this time, our investigation of other agencies is not complete

4. Conclusion:

SPA's experiences with the Departments of Defense and Labor leave it with the impression that the government's house is not in complete order when it comes to making sure that government agencies are in compliance with federal copyright laws. SPA concurs with the recommendation of the Defense Department's Inspector General that only a strong message delivered from the top will operate to encourage all government agencies and their

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 55 1999

component parts that only authorized software should be used on government computers. The U. S. Government must declare itself a "piracy free zone" for computer software. Only then, can it hold itself out to the rest of the world as a model abider of intellectual property laws.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 56 1999

TAB 2

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 57 1999



Audit Report

OFFICE OF THE INSPECTOR GENERAL

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

Report Number 93-056 February 19, 1993

Department of Defense

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 58 1999

The following acronyms are used in this report.

7CG.....Air Force 7th Communications Group
ADPE.....Automated Data Processing Equipment
ASD(C3I).....Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
DASD(IS).....Deputy Assistant Secretary of Defense (Information Systems)
DTSA.....Defense Technology Security Administration
LAN.....Local Area Network
MDW.....U.S. Army Military District of Washington
MOU.....Memorandum of Understanding
NAVAIR.....Naval Air Systems Command
SPA.....Software Publishers Association
USAISC.....U.S. Army Information Systems Command

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 59 1999

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

February 19, 1993

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
INSPECTOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Controls Over Copyrighted Computer Software (Report No. 93-056)

This is our final report on controls over copyrighted computer software. The report identifies a significant level of unauthorized use of copyrighted software on computers throughout the Department of Defense.

A draft of this report was issued to the addressees for comment on September 30, 1992. Comments from the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) were received on November 25, 1992, and from the Department of the Army on October 19, 1992.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred with the conditions described in the report but nonconcurred with the recommendations to alleviate the conditions on the premise that existing laws and Federal regulations require copyrighted software to be controlled. In view of the pervasion of the condition disclosed by the audit and for the specific reasons provided in the Audit Response section in Part II of the report, we request that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) reconsider the need for corrective action in this matter and provide additional comments in response to this final report.

The Army concurred with the finding and the recommendations in the draft report. The Departments of the Navy and Air Force did not reply to the draft report. While not required, the Navy and Air Force are invited to comment on the final report.

DoD Directive 7650.3 requires that all audit recommendations be resolved promptly. Recommendations are subject to resolution in accordance with the Directive in the event of nonconcurrence

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 60 1999

or failure to comment. Therefore, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) must provide final comments on the unresolved recommendations within 60 days of the date of this report.

In view of the potential existence of the conditions discussed in this report throughout the Department, the distribution has been expanded, as shown in Appendix F, beyond that normally afforded our reports. Should recipients desire additional copies for distribution to subordinate activities, they can be obtained by contacting the office designated on the Table of Contents.

The courtesies extended to the audit staff are appreciated. If you have any questions on this audit, please contact Mr. Harrell D. Spoons, the Program Director, at (703) 692-2846 (DSN 222-2846) or Mr. Marvin L. Peek, the Project Manager, at (703) 692-2939 DSN (222-2939).



Robert J. Lieberman
Assistant Inspector General
for Auditing

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 61 1999

Office of the Inspector General, DoD

AUDIT REPORT NO. 93-056 **February 19, 1993**
(Project No. 2RF-5004)

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

EXECUTIVE SUMMARY

Introduction. Copyrighted computer software programs are used on as many as 377,500 microcomputers throughout the DoD. DoD does not maintain records on the number of software programs on hand, but the proliferation of computers within DoD suggests that millions of software programs may be in use. Federal copyright law grants copyright owners exclusive rights to duplicate or distribute the programs. Although software vendors attempt to control unauthorized use of their products through licensing agreements that invoke the protection available under copyright statutes, compliance with licensing agreements relies on the integrity of the software user.

Objective. The audit objective was to determine whether policies and procedures for controlling and using computer software programs within the DoD were adequate to ensure compliance with licensing agreements and copyrights. We also evaluated applicable internal controls.

Audit Results. The audit showed that 51 percent of the 1,022 computers tested had copyrighted software programs installed without documentation to prove that the software had been legally acquired. Unauthorized use of copyrighted computer software contravenes Federal laws and denies software vendors their rightful revenues.

Internal Controls. We found material weaknesses in the internal controls designed to monitor the installation and accountability of copyrighted computer software programs. The controls we assessed are described in Part I of the report, and the finding provides details on the weaknesses.

Potential Benefits of Audit. No monetary benefits are associated with the recommendations in this report. Implementation of the recommendations will strengthen controls over the use of copyrighted software and reduce the risk of copyright infringement in the DoD. A summary of benefits resulting from this audit is in Appendix D.

Recommendations. We recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) issue better guidance, requiring all DoD Components to establish and enforce controls over the use and accountability of copyrighted computer software. No recommendations were directed to the

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 62 1999

Military Departments. However, because the conditions disclosed by the audit were prevalent throughout the DoD, the report was addressed to the Military Departments to provide an opportunity to comment on the results of the audit.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred with the finding, but nonconcurred with the recommendations, stating that existing laws and regulations are already in place. We believe the Assistant Secretary needs to provide leadership by issuing stronger and more explicit guidance on the need for better internal controls.

The Army concurred with the finding and the recommendations; the Navy and the Air Force did not provide comments. The complete texts of managements' comments are in Part IV. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) should provide comments on the unresolved issues within 60 days of the date of this report.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 63 1999

TABLE OF CONTENTS

	Page
TRANSMITTAL MEMORANDUM	
EXECUTIVE SUMMARY	i
PART I - INTRODUCTION	1
Background	1
Objectives	2
Scope	2
Internal Controls	3
Prior Audits and Other Reviews	3
Other Matters of Interest	4
PART II - FINDING AND RECOMMENDATIONS	7
Controls Over Copyrighted Software	7
PART III - ADDITIONAL INFORMATION	19
Appendix A - Summary of Army Audit Agency Reports on Computer Software Management	21
Appendix B - Summary of Air Force Audit Agency Reports on Small Computer Software Management	25
Appendix C - Sample Memorandum of Understanding for Users of Commercial Software	27
Appendix D - Summary of Potential Benefits Resulting from Audit	29
Appendix E - Activities Visited or Contacted	31
Appendix F - Report Distribution	33
PART IV - MANAGEMENT COMMENTS	37
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)	39
Department of the Army	43

This report was prepared by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, DoD. Copies of the report can be obtained from the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate (703) 614-6303 (DSN 224-6303).

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 64 1999

PART I - INTRODUCTION

Background

At the end of FY 1991, DoD activities reported having about 377,500 automated data processing equipment (ADPE) systems on hand that cost less than $15,000 each. Only summary records were reported for ADPE systems costing less than $50,000; therefore, the audit assumed that ADPE systems costing less than $15,000 were primarily microcomputers. DoD does not maintain an overall inventory of computer software, and no reliable estimates were available indicating the cost to purchase software for microcomputers within DoD. However, since microcomputer users rely almost exclusively on commercially developed, off-the-shelf software programs and since multiple software programs are common on each microcomputer, it is reasonable to assume that millions of commercially developed software programs are installed on microcomputers in DoD. Because of the wide variance in the cost of popular commercial software programs, we could make no meaningful estimate concerning the total cost of software installed on DoD microcomputers.

Software vendors attempt to control unauthorized use of their products through license agreements that invoke the protection available under Federal copyright statutes. The specific license agreement for each software product is explained in documentation accompanying the system disks that enable the user to install and operate software programs on a computer. Although the wording may differ slightly, license agreements specify that each software program purchased is to be used on one computer at a time. In some instances, an activity may purchase a "site license" or a license to use a software program on a local area network (LAN) of computers. Such licenses permit an activity to use the covered software program on the number of computers stated in the agreement. Most vendors have chosen not to incorporate built-in controls to disable software when it is copied; therefore, compliance with license agreements relies on the integrity of the software user.

U.S.C., title 17, section 106, gives owners of copyrights the exclusive rights to reproduce, distribute, or make derivative works of their material. Section 504 of the statute states that a copyright infringer is liable for actual damages to a copyright owner or statutory damages up to $100,000. The Defense Federal Acquisition Regulation Supplement, paragraph 252.227-7013, also provides provisions for commercial software purchased by DoD activities. In summary, the provisions state that ownership of the software remains with the contractor (i.e., copyright holder), and the Government has the right to use software in the computer for which the software was acquired.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 65 1999

Organizations within the computer software industry, such as the Software Publishers Association (SPA), have heightened public awareness of software copyright requirements. The SPA is fighting software piracy through a three-way approach of litigation, education, and public relations. Settlements reached with companies accused of software piracy range into the hundreds of thousands of dollars. The audit did not identify any litigation involving misuse of copyrighted software at any of the activities visited; however, U.S.C., title 28, section 1498, states that owners of commercial software copyrights can take action against the Federal Government for copyright infringement.

Objectives

The overall objective of the audit was to determine whether policies and procedures for controlling and using computer software programs within DoD were in accordance with licensing agreements and copyrights. Specifically, we determined whether the DoD activities audited were complying with copyright laws and licensing agreements, and we evaluated internal controls over copyrighted software.

Scope

The audit included a review of each Military Department's guidance on controls over copyrighted software and the implementing procedures in use at the subordinate commands and activities audited. We physically examined a judgmental sample of computers at each activity to determine whether the software installed on microcomputers was supported by documentation showing that it had been legally acquired. We examined 1,022 computers in 22 activities within the Military Departments. The sample was limited to IBM[1]-compatible computers. At the time of the audit, over 90 percent of the microcomputers within DoD were IBM-compatible. Records pertaining to software procurement, accountability, and inventories were examined when such records were maintained. We also reviewed audit reports and management reports related to software management that were issued from FY 1987 through FY 1991 by the Military Department audit agencies and other organizations responsible for controls over software.

This program audit was made from December 1991 through June 1992 in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD, and accordingly included such tests of internal controls as were considered necessary. Activities visited or contacted are listed in Appendix E.

---

1 IBM is a registered trademark of the International Business Machines Corporation.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 66 1999

Internal Controls

The audit identified material internal control weaknesses as defined by Public Law 97-255, Office of Management and Budget Circular A-123, and DoD Directive 5010.38. Controls either had not been established or were not adequate to ensure compliance with software licensing agreements. Furthermore, some activities did not maintain records of software procurement or accountability that were adequate to verify that computer software was legally acquired. Details on the internal controls we reviewed and the weaknesses we found are described in the Finding. All the recommendations in this report, if implemented, will correct the weaknesses. No quantifiable monetary benefits will be realized by implementing the recommendations; however, increased emphasis on compliance with software licensing agreements should help prevent violations of copyright laws, possible litigation against the Government, and resulting fines and penalties. A copy of this report will be provided to the senior officials responsible for internal controls within the Office of the Secretary of Defense and the Army, Navy, and Air Force.

Prior Audits and Other Reviews

Inspector General, DoD, Audit Report No. 92-092, "Alleged Misuse of 'SGT Security' Commercial Software," May 15, 1992, evaluated the merits of an allegation that the Air Force 7th Communications Group illegally copied and used "SGT Security" software. The allegation could not be substantiated. The report contained no recommendations.

Inspector General, DoD, Audit Report No. 92-134, "Controls Over Copyrighted Computer Software at the Defense Technology Security Administration," (DTSA) September 9, 1992, showed that DTSA had violated licensing agreements by installing copyrighted computer software that had not been purchased and had not maintained adequate documentation for other software installed. The report recommended that DTSA identify and remove unauthorized software and establish internal controls over the acquisition and use of copyrighted software. Management concurred with the finding and recommendations and initiated corrective actions.

The Army Audit Agency issued five installation reports as a result of one multilocation audit. The audit found that 41 percent of the computers sampled had undocumented commercial software installed. The audit also found that commercial software was not properly accounted for or controlled and that policies governing the control and use of software installed on Army-owned computers had not been established. Two summary reports were issued in 1989 as a result of that audit. Two other audits that included Army activities in Europe and Army Reserve activities had similar findings. Details on the Army Audit Agency reports are in Appendix A. We found similar deficiencies

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 67 1999

at Army organizations we audited. Audit results at one of the installations, Headquarters, Information Systems Command, for which a report had been issued by the Army Audit Agency, are shown in the Finding of this report.

Although no Air Force-wide audits of controls over computer software have been conducted, the Air Force Audit Agency issued 33 reports on individual installations from FY 1987 through FY 1991. Of the 33 reports, 28 showed that software had been installed without documentation to show that it had been legally acquired. The reports recommended removing unauthorized software, maintaining and reconciling software inventory records, and performing random reviews to ensure only authorized software is installed. The Air Force Audit Agency performed follow-up audits for 4 of the 33 reports. Three of the follow-up reports showed that corrective actions had not been taken. A summary of the reports is provided in Appendix B. We audited two activities at Dover Air Force Base, Delaware, for which the Air Force Audit Agency had issued reports. The 436th Logistics Support Squadron had implemented the audit recommendations, and all computers tested at that activity had documentation supporting the software that was installed. The 436th Military Airlift Wing had not implemented the audit recommendations.

Other Matters of Interest

Demonstration software. Software manufacturers sometimes provide individuals or organizations software for use on a trial basis. The capabilities of the software and the terms and conditions for use vary. Some demonstration software is fully functional only for a limited time. Other demonstration software is fully functional, and software vendors may ask that it be returned if it is not purchased. In other cases, the software may be provided free. Irrespective of the terms or conditions of use, it is important that the use and particularly the return of demonstration software is documented. As part of this audit, we reviewed allegations by a software manufacturer that the Air Force 7th Communications Group (7CG) failed to return the original copy of a demonstration software program and made illegal copies of the program.[2] The allegation was not substantiated; however, the 7CG had not implemented procedures to document the receipt and return of demonstration software. Although such procedures may not have prevented the allegation, documentation of the return of the software would have appreciably reduced the efforts expended in determining the validity of the allegation.

Shareware. Shareware is user-supported software or "try before you buy" software that is normally distributed free of charge through computer bulletin boards or advertisements in computer magazines. Shareware authors encourage users to give

2 Report No. 92-092, "Alleged Misuse of 'SGT Security' Software," May 15, 1992.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 68 1999

copies to others for evaluation as a way of advertising the product. The language used in shareware copyright notices has caused confusion about the need to pay for such software. For example, some copyright notices "encourage" users to register and remit a specific fee, and terms like "contribution" or "donation" are used to describe payment. Regardless of the language used, Code of Federal Regulations, title 37, states that Government entities that continue using shareware programs after the trial period must pay for such use. Here again, documentation is important to show the use or disposition of the software to avoid perceptions of or actual misuse.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 69 1999

PART II - FINDING AND RECOMMENDATIONS

CONTROLS OVER COPYRIGHTED SOFTWARE

Unauthorized software had been installed on 51 percent of 1,022 computers tested. This condition existed because controls to ensure compliance with computer software licensing agreements and copyright laws were either ineffective or nonexistent and because of management indifference. Unauthorized copying, dissemination, and use of copyrighted computer software in DoD contravenes Federal law, denies copyright owners their rightful revenues, and exposes the DoD to potential litigation and public discredit.

DISCUSSION OF DETAILS

Guidance

DoD. DoD Instruction 7920.5, "Management of End User Computing," March 1, 1989, states that it is DoD policy to enforce the licensing provisions of commercial software. The Instruction tasks DoD Component heads with ensuring compliance with the terms and conditions of copyright and licensing agreements. Additionally, "Defense Ethics," a guide for DoD employees published in January 1989 by the Inspector General, DoD, states:

> Vendor software may not be reproduced for distribution, other than to authorized Government agencies, according to the terms and conditions of the contract. If you violate copyright laws and other conditions of a software licensing agreement, you are acting on your own accord, and disciplinary action may be taken against you.

Army. Army Regulation 25-1, "Army Information Resources Management Program," November 18, 1988, states that proprietary software must be protected by the user/accountable individual from unauthorized use, abuse, or duplication. Although formal property book accountability is not required, software is to be controlled as a durable, receipted item. However, the Regulation does not specify that software should be traced to a specific computer, and the audit showed that receipts had been prepared for multiple copies of software without identification of the computers on which the software was authorized to be installed.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 70 1999

Five of the seven Army activities audited had issued local guidance emphasizing the need to comply with software licensing agreements and copyright laws. Two major command headquarters that we audited, U.S. Army Information Systems Command (USAISC) and U.S. Army Military District of Washington (MDW), issued regulations requiring that annual inventories of software be made for accountability and control and that original software diskettes be maintained by authorized users for auditing purposes. The regulations also required that each software user sign a Memorandum of Understanding (MOU) (see Appendix C) that summarized the provisions of the software licensing agreements. However, the audit showed that the MOUs were not being used by the organizations audited within those two command headquarters. To be effective, controls must be implemented and enforced.

Navy and Marine Corps. At the time of the audit, no Navy-wide instructions regarding controls over copyrighted computer software had been issued. However, a Secretary of the Navy instruction was being prepared that would address controls over copyrighted software. Among the Navy's major commands, only the Naval Air Systems Command (NAVAIR) had issued instructions governing the use of copyrighted software. NAVAIR Instruction 5239.1, "Software Duplication Policy," December 20, 1985, states that it is NAVAIR policy not to make copies of copyrighted software unless authorized in writing by the copyright owner. During the audit, the Naval Facilities Engineering Command published a similar instruction, but only three of the four Navy field activities audited had issued guidance that emphasized the importance of complying with software licensing agreements. However, none of the instructions addressed how software should be accounted for or controlled.

The Marine Corps Small Computer Systems Security Manual (the Manual), May 23, 1990, states that making unauthorized copies of software is a violation of copyright laws and that employees are subject to indictment and conviction if found guilty. Further, the Manual recommends conducting periodic software inventories and requiring users to sign a document acknowledging they are prohibited from making unauthorized copies. Furthermore, "White Letter" No. 4-90, "Computer Viruses," June 29, 1990, issued by the Commandant of the Marine Corps, prohibits the use of copied or pirated software.

Air Force. Air Force Regulation 700-26, "Management of Small Computers," December 15, 1988, summarizes copyright laws, stating that copying commercially purchased software without a license agreement is illegal. The Regulation requires that an inventory of the software installed on each computer be maintained. Although the Regulation requires software accountability at the user level, the audit showed that the requirement for inventories was not enforced at the activities audited. For example, guidance issued by Headquarters, Air Force Logistics Command, required that a "software control log" be established for each computer system. However, the guidance to

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 71 1999

establish accountability was not followed. Furthermore, only four of the seven Air Force activities audited had issued implementing guidance.

Review of Software on Computers

The audit showed that unauthorized software had been installed on computers at each of the 22 Military Department activities audited. This condition existed even though each activity was given prior notice of the purpose and date of the audit. Each activity had ample opportunity to remove unauthorized software from their computers, and some commands had directed such removal. The results of the audit tests are shown Tables 1., 2., and 3. below.

Table 1. Results of Computers Tested - Army

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Headquarters, Army Staff	53	28	78
Headquarters, Information Systems Command, Fort Huachuca	45	16*	33*
Headquarters, Military District of Washington, Fort McNair	30	13	23
Headquarters, Army Depot System Command	19	7	12
Fort Belvoir	76	61	136
Fort Bragg	68	46	199
Letterkenny Army Depot	62	34	84
Totals	353	205	565

* On August 26, 1992, USAISC informed us that documentation had been located for all but 12 undocumented software programs we found during our audit. We did not verify the information since it was provided after our visit to USAISC.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 72 1999

Table 2. Results of Computers Tested - Navy and Marine Corps

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Navy			
Headquarters, Naval Air Systems Command	31	16	57
Headquarters, Naval Facilities Engineering Command	37	19	58
Headquarters, Naval Supply Systems Command	31	9	15
Naval Command, Control, and Ocean Surveillance Center; Research, Development, Test, and Evaluation Division	44	30	79
Naval Supply Center, San Diego	42	31	85
Norfolk Naval Shipyard	71	33	56
Public Works Center, San Diego	62	24	47
Marine Corps			
Central Design and Program Activity, Quantico	48	8	10
Totals	366	170	407

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 73 1999

Table 3. Results of Computers Tested - Air Force

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Headquarters, Air Staff	60	31	109
Headquarters, Air Force Logistics Command	42	25	59
Headquarters, Tactical Air Command	52	14	24
1st Tactical Fighter Wing, Langley Air Force Base	30	30	116
7th Communications Group	35	4	6
2750th Airbase Wing, Wright-Patterson Air Force Base	41	29	64
Dover Air Force Base	43	17	31
Totals	303	150	409

None of the officials at the audited activities could provide evidence to show that a total of 1,381 copyrighted software programs installed on 525 (51 percent) of the 1,022 computers tested had been legally acquired. We estimated the retail value of the unauthorized software programs at about $227,000.

Undocumented software. Computer users offered various reasons why undocumented software was installed on the computers tested. From the reasons cited, it was evident that the problem stemmed from ineffective or nonexistent controls and a lack of management emphasis on compliance with licensing agreements. For example, computer users claimed they were unaware of certain software programs installed on their computers, that the software was already installed on computers when they were assigned, that software documentation had been lost, or that they were unaware of or did not understand copyright restrictions.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 74 1999

Controls. The relatively low cost of software programs intended for use on microcomputers, the need to make backup copies of system disks, and the ease of illegally duplicating disks create a daunting control challenge. However, effective controls are essential to ensure compliance with software licensing agreements and Federal copyright statutes. The following examples show that controls ranged from reasonably effective to nonexistent among the activities audited.

o The Training Management Section, 436th Logistics Support Squadron, Dover Air Force Base, developed effective procedures to control and account for all software installed on its computers. A custodian maintained an inventory of all software installed on the 15 computers within the Training Section. He also maintained the original diskettes, by computer serial number, in a central location. No undocumented software was found on the eight computers tested at the Training Section. The Training Section had been included in a software audit by the Air Force Audit Agency in 1990 and had implemented recommendations resulting from that audit.

o The Resource Management Directorate, Headquarters, U.S. Army Depot System Command, had developed procedures to account for software and to inform users of their responsibilities. An inventory of the software installed on each computer was maintained with the machines. Additionally, original diskettes, bar coded to identify the computer on which the software was installed, were kept locked in a storage cabinet. Supervisors, managers, and computer users were required to attend an annual Automation Security Briefing, reminding them of local policies and of software copyright restrictions. Those personnel were required to sign a form acknowledging their responsibilities and their understanding of policies and procedures for automation security and controls over computer software. Each individual was also given a reference copy of the policies and procedures. Only 1 unauthorized software program was installed on the 10 computers tested.

o After being notified of the audit, the 7th Communications Group (7CG) instructed computer users to remove all software that could not be supported by purchase documentation. The 7CG also provided each user and the Computer Systems Security Officer a list of the software authorized on each computer. Each user was to maintain the original software and documentation. These procedures to control and account for software were established in a 7CG instruction published during the audit. The audit tested 35 computers and found 6 unauthorized software programs.

o At one Army unit, the software on the computers had not been inventoried and was not identified on receipts at the user level. Users could not provide reasons why unauthorized software was installed on their computers. During our exit briefing, the unit commander stated most users probably assumed

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 75 1999

that all software was "owned" by the Army and could be used and copied freely. The audit tested 10 of 27 computers and found 76 unauthorized software programs.

o An Air Force squadron branch had issued an Operating Instruction that stated, "It is generally illegal to make several copies of one original software product then run the copies on different systems." However, the branch chief stated he understood that only one copy of each software package in use needed to be purchased. He indicated that individual software programs that had been purchased were copied to the majority of computers in the branch. The audit tested 8 of 14 computers and found 44 unauthorized software programs installed.

Documentation. Records at some activities were not adequate to show that software had been legally acquired. For audit purposes, the original copyrighted software diskettes, site licenses, receipts, and accreditation packages showing specific software had been authorized were accepted as evidence of legal ownership. When documentation was available to establish ownership of a software program, the audit treated all copies of the software as authorized, up to the quantity for which ownership had been established, even though records did not identify the specific computer on which the software was installed. We questioned 421 software programs because no records were available to show where the software was authorized to be installed, but we did not count those programs as unauthorized. However, since copyrighted software ordinarily may be used on only one computer at a time, knowledge of where each copy of a software program is installed is necessary to ensure compliance with the licensing agreement. The absence of such records highlights the lack of adequate internal controls over the use of copyrighted software.

o We tested 24 computers at one Army Headquarters Staff activity and were unable to determine whether 132 software programs installed were authorized, because accreditation packages with documentation for authorized software by computer were incomplete and frequently could not be matched to a specific computer.

o Software and supporting documentation for one Pentagon-based Air Force Headquarters Staff activity was maintained by a custodian located at Bolling Air Force Base. Because the custodian kept software for about 300 users, the volume of material required that the software and documentation be stored at three separate locations. None of the software was identifiable to a specific computer or user. The custodian kept the software documentation because users complained that it took up too much space.

At some of the activities audited, personnel claimed that software may have been purchased, but diskettes and manuals, which provide evidence of software ownership, had been lost. For

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 76 1999

example, when undocumented software was found at one unit at Fort Bragg, the Commander stated that software documentation was lost during the buildup for Operation Desert Shield and the deployment for Operation Desert Storm.

The audit showed that there were fewer instances of unauthorized software when computers were operated on a LAN. However, even though LANs eliminate the need for installing most software programs on individual computers, the following examples show that controls are still needed to guard against unauthorized software.

o Computers at one section of the Navy Public Works Center, San Diego, were connected to a LAN. Only two designated personnel were authorized to install or remove software. Software approved for installation on the LAN was stored in a central location and could be easily inventoried. If additional software was approved, it was maintained with the specific user for whom it had been authorized. The audit tested 17 computers and found only 3 unauthorized software programs.

o The Marine Corps Central Design and Programming Activity's computers were connected to a LAN. Most of the activity's authorized software was installed on the LAN rather than on the hard drives of individual computers. The audit tested 48 computers and found only 10 unauthorized software programs.

Management emphasis. Computer security officers interviewed during the audit reported that efforts to control copyrighted computer software were hampered by a lack of command emphasis on the importance of complying with copyright laws and licensing agreements. The problem is illustrated by the following examples.

o The Chief of Staff at one Army activity stated that because software has minimal value, the command could not afford to expend the hours needed to account for every software program. In his opinion, most software should be considered a consumable item without a requirement to account for it.

o The computer security officer at one Navy command credited the audit with helping the command's senior management to recognize that a problem existed. After the audit, the command began an extensive review of software needs and developed plans to purchase the necessary software to ensure compliance with software licensing agreements.

o At one Air Force activity where unauthorized software was installed on computers, personnel reported that they were frequently required to respond to senior management taskings using specific software programs even though the software had not

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 77 1999

been purchased. The deputy director of the activity stated that he had verbally advised senior management of this problem, but the practice continued.

o Within 1 section of an Air Force squadron, we tested 12 of 20 computers and found 21 unauthorized software programs. The squadron commander knew that unauthorized copies of software programs in excess of the quantities purchased had been installed on the squadron computers. He stated that due to insufficient funds, the required number of copies of the software could not be purchased, but that the software programs were needed for the squadron's mission and the mission came first.

Conclusions

The audit results cannot be statistically projected because the sample was judgmental; however, the results are sufficient to show that licensing agreements for copyrighted computer software were ignored at all levels of command in each Military Department. Taken together with similar results reported by the Army and Air Force Audit Agencies (see Appendixes A and B), the audits present compelling evidence that abuse of software licensing agreements has been and remains commonplace throughout DoD. Most significantly, the audit showed that leaders and managers have not only acquiesced in the continuing abuse of software licensing agreements, but that they have directed actions that required violation of Federal copyright statutes. Disregard of Federal law under the guise of expediency signals an unacceptable breakdown in integrity and ethical behavior among those who are responsible.

The public has a right to expect honest and fair treatment when dealing with the DoD. It is incumbent on all public servants, both military and civilian, that the highest standards of ethical behavior and personal integrity be maintained in all official matters. Senior leaders must demand and enforce the highest standards of conduct, and potential copyright infringers must be assured that improper acts will be dealt with appropriately.

Formal controls over copyrighted computer software and formal procedures for implementing the requisite controls are necessary to ensure that leaders, managers, and computer users know and apply needed safeguards to preclude copyright infringement. The needed guidance has not been issued at all activities. Furthermore, the audit showed that, with rare exception, existing guidance was generally ignored by the activities audited. Controls need not be onerous; management enforcement is the key to effectiveness. Unauthorized software should be prohibited. In order to negate any future allegation of copyright infringement, proof of legal possession of copyrighted software and a record to show on which computer the software is installed should be retained for as long as the software is used.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 78 1999

RECOMMENDATIONS FOR CORRECTIVE ACTION

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issue guidance requiring DoD Components to:

1. Inform all personnel of copyrighted computer software licensing agreements and of the potential consequences for copyright infringement.

2. Prohibit the possession or use of unauthorized copyrighted computer software, and administer disciplinary action for any circumvention.

3. Establish controls to ensure that proof of legal possession of copyrighted computer software is retained for as long as the software is used.

4. Establish procedures to identify copyrighted computer software that is authorized to be installed on each computer.

MANAGEMENT COMMENTS AND AUDIT RESPONSE

Management comments. In responding for the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) the Deputy Assistant Secretary of Defense (Information Systems) (DASD[IS]) concurred with the finding, but nonconcurred with the recommendations. The DASD(IS) also doubted that the majority of the incidents of improperly documented software were the result of willful violations of copyright laws. The complete text of the comments is in Part IV of the report.

The DASD(IS) stated that existing laws and Federal regulations, as cited in the draft report, already have established the requirement to control copyrighted software. Thus, the problem is noncompliance with, rather than a lack of, laws and regulations. The comments suggested noncompliance could be addressed as part of routine IG, DoD, inspections and audits.

The response stated that the problem will get more visibility because the DASD(IS) Information Management Self-Assessment Guide addresses the extent to which DoD Components have implemented internal controls to preclude the unlawful copying of copyrighted software. Also, DASD(IS) officials are evaluating the feasibility of including language regarding copyrighted software in future DoD directives or instructions, but in the interim, they are satisfied with existing policy in DoD Instruction 7920.5, "Management of End User Computing." The Instruction tasks Component heads to "Ensure compliance with the terms and conditions for commercial software use, including copyright and license agreements."

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 79 1999

The DASD(IS) suggested minor changes to the draft report section entitled "Prior Audits and Other Reviews," regarding violations on licensing agreements at the Defense Technology Security Administration and corrective actions taken.

Audit response. We agree with the DASD(IS) that the major cause of violations of licensing agreements and copyright laws is noncompliance with existing laws and regulations. However, the audit showed that existing DoD and Military Department guidance was not effective in preventing abuse of copyrighted software licensing agreements. DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I])," February 12, 1992, makes the ASD(C3I) the principal DoD official responsible for establishing software policy and practices. The ASD(C3I) has not promulgated policy guidance stressing the need for all management levels to ensure compliance with software licensing agreements. Given the audit evidence that abuse of software licensing agreements within DoD is commonplace, management's comment that it is "satisfied with existing policy" reinforces the overall impression of management indifference to the abuse of software licensing agreements.

The Software Copyright Protection Act (Public Law 102-561) was signed by the President on October 28, 1992. The Act provides penalties of up to 5 years in prison and fines of up to $250,000 for persons infringing on at least 10 copies of a copyrighted software program or any combination of programs with a retail value greater than $2,500. Had that law been in effect during the audit, referrals to criminal investigative activities would have been necessary. We believe the criminal penalties need to be brought to the attention of all DoD managers and microcomputer users.

Audit recommendations were not addressed to the DoD Components because we believe the ASD (C3I) must lead on this issue. Guidelines directed to the data processing and information management technical communities will not suffice. Our audit recommendations focus on what DoD Components should do to "ensure compliance with the terms and conditions of commercial software use...." as stated in DoD Instruction 7920.5. The recommendations also emphasize the need to establish controls and procedures to identify software authorized to be installed on computers. If these procedures are not established, DoD activities will not be able to determine whether they are in compliance with software licensing agreements, and disciplinary actions cannot be administered for noncompliance.

DASD(IS) personnel provided us a copy of the Information Management Self-Assessment Guide, dated November 25, 1992. The Guide helps implement DoD Instruction 7740.3, which requires DoD activities to conduct periodic reviews of their information management installations. The Guide contains 141 internal control questions on 17 functional areas. Three of the questions relate to controls over copyrighted computer software. While the

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 80 1999

Guide is helpful, we believe that three questions on software controls buried in an overall information management guide do not constitute the emphasis senior DoD management should convey to correct the problem.

Changes in the wording of the "Prior Audits and Other Reviews" section were made in the final report based on management's comments. However, our comments regarding corrective actions by the Defense Technology Security Administration (DTSA) (Report No. 92-134) were not changed. Our report stated that DTSA had initiated corrective actions. We did not state that DTSA had taken corrective actions, since we did not verify actions taken after the audit was completed.

We consider management's comments to be nonresponsive because no corrective action is planned. For the reasons cited above and in the details of the conditions, we maintain that the audit recommendations are still valid. However, we have changed the wording of the recommendations from requiring a "DoD Directive" to requiring "guidance," so that management has more flexibility in responding to the need for demonstrating a stronger interest in establishing proper internal controls in this area. We agree that DoD oversight organizations will have an important role in monitoring compliance with those controls, but management should not wait for further reports of noncompliance with the law to take corrective and preventative action. We request that the ASD(C3I) reconsider the matter and provide comments on each recommendation in response to this final report.

Other Comments. The Army concurred with the recommendations. The Navy and the Air Force did not provide comments to the draft report. Should they desire, the Navy and Air Force may respond to this final report.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 81 1999

PART III - ADDITIONAL INFORMATION

Appendix A - Summary of Army Audit Agency Reports on Computer Software Management

Appendix B - Summary of Air Force Audit Agency Reports on Small Computer Software Management

Appendix C - Sample Memorandum of Understanding for Users of Commercial Software

Appendix D - Summary of Potential Benefits Resulting From Audit

Appendix E - Activities Visited or Contacted

Appendix F - Report Distribution

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 82 1999

APPENDIX A: SUMMARY OF ARMY AUDIT AGENCY REPORTS ON COMPUTER SOFTWARE MANAGEMENT

The U.S. Army Audit Agency conducted three multilocation audits from March 1988 through December 1990, covering the acquisition, use, control, and accountability of commercial software.

One multilocation audit resulted in five installation reports that were consolidated into the two summary audit reports listed below. The problems and suggested corrective actions were also reported in two advisory reports with the same titles.

- Report No. SW 89-209, "Commercial Software Copyrights," May 29, 1989

- Report No. SW 89-208, "Acquisition, Use, and Control of Commercial Software," June 12, 1989

The Army Audit Agency found that:

- Policies and procedures had not been established to prevent, detect, or control unauthorized copying of commercial software.

- Policies and controls were not adequate to ensure that commercial software was properly accounted for and controlled.

- The Army Internal Control Program, as it relates to the acquisition, use, and control of commercial software was not adequate.

Based on a statistical sample:

- 41 percent of the Army-owned "personal" computers had undocumented copies of commercial software valued at $21 million;

- $43 million in software disks and documentation were improperly secured;

- 43 percent of the computers had unapproved shareware and "freeware"; and

- 18 percent of the computers had software acquired by personnel.

The Army Audit Agency found that the planning, justification, and approval process for the acquisition of commercial software and training programs for commercial software users were inadequate. Also, inadequate guidance had been issued for handling lost,

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 83 1999

APPENDIX A: SUMMARY OF ARMY AUDIT AGENCY REPORTS ON COMPUTER SOFTWARE MANAGEMENT (cont'd)

stolen, damaged, or excess software; registering software; and safeguarding software. These areas were not included in the scope of our audit.

The Army Audit Agency recommended that policies and procedures be established to:

- Deal with past potential copyright infringements by identifying undocumented commercial software and establishing a contingent liability.

- Inform users of their responsibilities to honor software copyrights.

- Require periodic reviews of computer hard drives to identify undocumented software.

- Discipline personnel when copyright infringements are identified.

- Physically safeguard software.

- Control shareware, "freeware," and privately owned software.

- Account for commercial software.

- Require annual physical inventories of all software and its documentation, and reconcile inventoried software with quantities recorded in property books.

Report No. SW 89-208 also recommended that the internal control checklists be revised, that guidance be furnished to information managers on their internal control responsibilities related to commercial software, and that a tracking system be developed to identify material weaknesses concerning commercial software.

The Army agreed that software was undocumented. However, based on advice from the Army General Counsel, the Army disagreed with the results of the statistical sample and the need for a contingent liability. The Army issued an Army-wide message in February 1989, directing local organization or installation managers to ensure compliance with copyright policy and to advise and assist customers who may not be familiar with the software copyright laws and agreements.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 84 1999

APPENDIX A: SUMMARY OF ARMY AUDIT AGENCY REPORTS ON COMPUTER SOFTWARE MANAGEMENT (cont'd)

Two other multilocation audits had similar findings and recommendations:

- Report No. EU 89-309, "Commercial Automation Software U.S. Army, Europe, and Seventh Army," May 1, 1989, states that accountability controls over commercial software, worth about $3.4 million, were not adequate.

- Report No. NE 91-300, "Acquisition, Use, and Maintenance of Automatic Data Processing Equipment and Software, 94th U.S. Army Reserve Command," April 12, 1991, states 89 percent of computers tested at four Army Reserve centers had undocumented software.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 85 1999

APPENDIX B: SUMMARY OF AIR FORCE AUDIT AGENCY REPORTS ON SMALL COMPUTER SOFTWARE MANAGEMENT

The Air Force Audit Agency issued 33 reports from FY 1987 through FY 1991 on small computer software management and 4 follow-up reports. The reports included reviews of 3 major command headquarters (Military Airlift Command; Air Force Communications Command; and U.S. Air Forces, Europe) and 30 bases or activities. The majority of the audit reports identified the following deficiencies.

- Unauthorized copyrighted software was found on computers tested (28 of 33 reports).

- Required software inventories were not maintained on computers tested (23 of 33 reports).

- Excess software was not properly identified and turned in for reutilization (16 of 33 reports).

- Software was not adequately safeguarded (1[illegible] of 33 reports).

The recommendations to correct deficiencies varied, but generally stated:

- Remove unauthorized software from Government-owned computers.

- Perform random spot checks of computer hard drives and software inventory records to determine that only authorized software is installed.

- Maintain software inventory records, and reconcile records periodically with original documentation to identify and resolve discrepancies.

- Provide adequate training to accountable personnel to ensure excess software is turned in for redistribution. Perform random spot checks to ensure compliance.

- Make backup master copies of software programs, and store diskettes in acceptable containers and areas.

Only one of the four follow-up reports stated that the deficiencies identified had been corrected. At three activities (Headquarters, Military Airlift Command; Headquarters, Air Force Communications Command; and 375th Military Air Wing), procedures had not been fully implemented to remove unauthorized software from computers.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 86 1999

APPENDIX C: SAMPLE MEMORANDUM OF UNDERSTANDING FOR USERS OF COMMERCIAL SOFTWARE

MEMORANDUM OF UNDERSTANDING
BETWEEN
DEPUTY CHIEF OF STAFF FOR INFORMATION MANAGEMENT
PLANS DIVISION
AND
MDW USERS OF COMMERCIAL SOFTWARE

SUBJECT: Computer Software Protection Policy

1. I recognize that computer software for Government-owned information systems may be licensed for a variety of outside companies. MDW does not own this software or its related documentation. Unless specific permission has been granted by the software licensor, no user has the right to (a) copy or reproduce software (this does not apply to authorized backup copies, (b) copy or reproduce the software package's related documentation, or (c) allow the software to be used simultaneously by another user.

2. I understand that software will only be used in accordance with the software licensing agreement.

3. I understand that if I knowingly make, acquire, or use unauthorized copies of computer software, I may be subject to discipline according to the circumstances.

4. I understand that pursuant to Federal statute, illegal reproduction of commercial software for personal use is subject to civil damages up to $50,000 and criminal penalties to include fines and imprisonment in accordance with Title 17, United States Copyright Code 504 and 506.

5. I have read and understand the software protection policies of AR [Army Regulation] 380-19, paragraph 2-4, and MDW supplement 1 thereto, and will abide by them.

_____
SIGNATURE/DATE

_____
NAME/GRADE

_____
ORGANIZATION/TELEPHONE NO.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 87 1999

APPENDIX D: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

Recommendation Reference	Description of Benefit	Type of Benefit
1.	Compliance and Internal Controls. Ensures all personnel are aware of copyright restrictions and penalties for abuse of licensing agreements.	Nonmonetary
2.	Internal Controls. Eliminates possession and use of unauthorized software.	Nonmonetary
3.	Internal Controls. Requires procedures to account for copyrighted computer software while it is in use.	Nonmonetary
4.	Internal Controls. Requires procedures to preclude unauthorized use of copyrighted computer software.	Nonmonetary

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 88 1999

APPENDIX E: ACTIVITIES VISITED OR CONTACTED

Office of the Secretary of Defense

Assistant Secretary of Defense, (Command, Control, Communications, and Intelligence), Washington, DC
Deputy Assistant Secretary of Defense (Management Systems)

Department of the Army

U.S. Army Inspector General Agency, Washington, DC
Deputy Chief of Staff (Logistics), Washington, DC
Deputy Chief of Staff (Plans and Operations), Washington, DC
Director of Information Systems for Command, Control, Communications, and Computers, Washington, DC
U.S. Army Audit Agency, Alexandria, VA
U.S. Army Information Systems Command, Fort Huachuca, AZ
U.S. Army Military District of Washington, Fort McNair, Washington, DC
Fort Belvoir, VA
U.S. Army Depot System Command, Chambersburg, PA
Letterkenny Army Depot, Chambersburg, PA
Headquarters, XVIII Airborne Corps and Fort Bragg, NC

Department of the Navy

Naval Information Systems Management Center, Assistant Secretary of the Navy (Research, Development, and Acquisitions), Washington, DC
Naval Air Systems Command, Washington, DC
Naval Sea Systems Command, Washington, DC
Norfolk Naval Shipyard, Portsmouth, VA
Naval Supply Systems Command, Washington, DC
Naval Supply Center, San Diego, CA
Naval Facilities Engineering Command, Alexandria, VA
Navy Public Works Center, San Diego, CA
Naval Audit Service, Arlington, VA
Space and Naval Warfare Systems Command, Washington, DC
Naval Command, Control, and Ocean Surveillance Center, Research, Development, Test, and Evaluation Division, San Diego, CA
Naval Computer and Telecommunications Command, Washington, DC

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 89 1999

APPENDIX E: ACTIVITIES VISITED OR CONTACTED (Cont'd)

Department of the Air Force

Assistant Secretary of the Air Force (Acquisitions), Washington, DC
Judge Advocate General, Air Staff, Washington, DC
Chief of the Air Force Reserve, Washington, DC
Deputy Chief of Staff (Personnel), Washington, DC
Deputy Chief of Staff (Command, Control, Communications and Computers), Washington, DC
Deputy Chief of Staff (Logistics), Washington, DC
Civil Engineer, Air Staff, Washington, DC
Air Force Audit Agency, Washington, DC
Air Force Logistics Command, Wright-Patterson Air Force Base, OH
  2750th Air Base Wing, Wright-Patterson Air Force Base, OH
Tactical Air Command, Langley Air Force Base, VA
  1st Tactical Fighter Wing, Langley Air Force Base, VA
7th Communications Group, Washington, DC
436th Airlift Wing, Air Mobility Command, Dover Air Force Base, DE

Marine Corps

Marine Corps Computer and Telecommunications Activity, Quantico, VA
Marine Corps Central Design and Programming Activity, Quantico, VA

Specified Commands

Headquarters, Forces Command, Fort McPherson, GA

Defense Agencies

Defense Automation Resources Information Center, Defense Information Systems Agency, Alexandria, VA

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 90 1999

APPENDIX F: REPORT DISTRIBUTION

Office of the Secretary of Defense

Under Secretary of Defense Acquisition
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
  Director of Defense Information
  Deputy Assistant Secretary of Defense (Information Systems)
Assistant Secretary of Defense (Force Management and Personnel,
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (International Security Affairs,
Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Production and Logistics)
Assistant Secretary of Defense (Program Analysis and Evaluation
Assistant Secretary of Defense (Public Affairs)
Assistant Secretary of Defense (Reserve Affairs)
Comptroller of the Department of Defense
  Deputy Comptroller (Management Systems)
  Director, Management Improvement
  Deputy Comptroller (Program/Budget)
Director of Defense Procurement
Director, Defense Research and Engineering
  Deputy Director (Test Evaluation)
Director, Operational Test and Evaluation
Assistant to the Secretary of Defense (Atomic Energy)
Assistant to the Secretary of Defense (Intelligence Oversight)
Director, Defense Acquisition Regulations Council
  (OASD[P&L], DASD[P]/DARS)
Assistant to the Secretary of Defense (Intelligence Policy)
Director, Administration and Management

Joint Staff

Director, Joint Staff
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command
Commander in Chief, U.S. Forces Command

Department of the Army

Secretary of the Army
Director of Information Systems for Command, Control, Communications and Computers
Inspector General, Department of the Army
Auditor General, Army Audit Agency

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 91 1999

APPENDIX F: REPORT DISTRIBUTION (Cont'd)

Department of the Navy

Secretary of the Navy
Assistant Secretary of the Navy (Financial Management)
Comptroller, Department of the Navy
Assistant Secretary of the Navy (Research, Development, and Acquisitions)
Commandant of the Marine Corps
Auditor General, Naval Audit Service

Department of the Air Force

Secretary of the Air Force
Assistant Secretary of the Air Force (Financial Management and Comptroller)
Deputy Chief of Staff, Command, Control, Communications and Computers
Auditor General, Air Force Audit Agency

Defense Agencies

Director, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
Director, Defense Investigative Service
Director, Defense Legal Services Agency
Director, Defense Logistics Agency
Director, Defense Mapping Agency
Director, Defense Nuclear Agency
Director, Defense Security Assistance Agency
Director, National Security Agency Central Security Service
Director, On-Site Inspection Agency
Director, Strategic Defense Initiative Organization

Non-DoD Activities

Office of Management and Budget
U.S. General Accounting Office
National Security and International Affairs Division, Technical Information Center
Software Publishers Association

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 92 1999

APPENDIX F: REPORT DISTRIBUTION (Cont'd)

Non-DoD Activities (Cont'd)

Chairman and Ranking Minority Member of Each of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Committee on the Judiciary
Senate Subcommittee on Patents, Copyrights, and Trademarks, Committee on the Judiciary
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations
House Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations
House Committee on the Judiciary
House Subcommittee on Courts, Intellectual Property, and the Administration of Justice, Committee on the Judiciary
House Committee on Science, Space, and Technology
House Subcommittee on Science, Research, and Technology, Committee on Science, Space, and Technology
House Permanent Select Committee on Intelligence
House Subcommittee on Oversight and Evaluation, Permanent Select Committee on Intelligence

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 93 1999

PART IV MANAGEMENT COMMENTS

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

Department of the Army

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 94 1999

ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGECE) COMMENTS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-3040

NOV 26 1992

MEMORANDUM FOR DIRECTOR, READINESS AND OPERATIONAL SUPPORT DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on Controls Over Copyrighted Computer Software (DoD Inspector General (DoDIG) Project No. 2RP-5004)

My staff has reviewed the subject draft audit report and circulated it to appropriate Components for comment.

We concur with the findings in the subject draft. The findings cannot be disputed, although we doubt that the majority of the incidents of improperly documented vendor proprietary software are a result of willful violations of copyright laws.

We do not concur with the recommendations. Existing laws and Federal regulations, as cited in the draft report, establish the requirement to control copyrighted software. The problem is not a lack of, but noncompliance with, existing laws and regulations, which could be addressed as part of DoDIG routine inspections and audits.

This problem will get more visibility in the future, because we have included a section in our Information Management Self Assessment Guide that addresses the extent to which Components have implemented internal controls to preclude the unlawful copying of copyrighted software. We are also evaluating the feasibility of including language regarding copyrighted software in future DoD Directives or Instructions; but in the interim, are satisfied with existing policy. DoD Instruction 7920.5, "Management of End User Computing," specifically tasks heads of Components to, "Ensure compliance with the terms and conditions for commercial software use, including copyright and license agreements." DoD 7740.1-G, "Department of Defense ADP Internal Control Guideline", July 1988, has a section on "Specific Microcomputer Control Considerations," which addresses this issue with the question, "Do policies prohibit the use of copyrighted and/or unauthorized software that the activity has not leased or purchased?"

The attachment to this memorandum contains recommended changes to the section on "Prior Audits and Other Reviews" in the Introduction of the draft report.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 95 1999

ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE) COMMENTS (Cont'd)

Should you have any questions regarding this response, my action officer is Tom May, at 703-746-7918.

Cynthia Kendall
Deputy Assistant Secretary of Defense
(Information Systems)

Attachment

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 96 1999

ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE) COMMENTS (Cont'd)

Draft Audit Report on Controls Over Copyrighted Computer Software (DoD Inspector General (DoDIG) Project No. 2RP-5004)

Page 5, Last paragraph:

Change "...DTSA had violated licensing agreements by installing copyrighted computer software that had not been purchased."

To read:"...DTSA had violated licensing agreements by installing copyrighted computer software for which purchase transactions had not been completed or for which adequate documentation could not be provided."

Rationale: The proposed wording provides an overall picture of the results of the DTSA Audit as it is reflected in report number 92-134, dated September 9, 1992. As stated on page 3 of the audit report, DTSA was found to have copyrighted software installed without documentation to show it had been legally acquired. At no time was there any finding that cites evidence of willful violation of the copyright laws. The recommended wording correctly states the findings.

Page 6, Continuation of last paragraph on page 5, last sentence:

Change: "Management concurred with the findings and recommendations and initiated corrective actions."

To read: "Management concurred with the recommendations and has taken corrective actions."

Rationale: While DTSA did not take exception to the general thrust of the findings, it did not necessarily concur with the wording of each finding or conclusion. As noted in Mr. Rudman's memorandum of August 14, 1992, DTSA "accepted its [the IG's] recommendations." Mr. Rudman also noted that the IG report does not cite evidence of willful violation of the copyright laws and that DTSA's own internal review did not reveal any such evidence (see pp. 19-28 of report number 92-134). Since Mr. Rudman's memorandum, DTSA has substantially completed implementation of the corrective actions recommended by the IG and the proposed language change reflects this progress.

Attachment

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 97 1999

DEPARTMENT OF THE ARMY COMMENTS

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
WASHINGTON, DC 20310-0107

Office, Director of Information Systems for Command, Control, Communications, & Computers

SAIS-IDP (36-2b) 19 Oct 92

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF ~~THE ARMY~~ Defense
~~ATTN: SAIG-PA (Mr. Flanagan),~~
~~WASHINGTON DC 20310-1700~~

SUBJECT: Draft Audit Report on Controls Over Copyrighted Computer Software (Project No. 2RF-5004)

1. Reference memorandum, SAIG-PA, 8 Oct 92, SAB, which forwarded for our review the draft DoD audit report.

2. We concur with all recommendations contained in the draft DoD audit report.

3. My point of contact is Mr. Arnold, (703) 614-0559.

FOR THE DIRECTOR:

LINDA S. DEAN
Deputy Director for Policy

CF:
SAIS-ADW

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 98 1999

AUDIT TEAM MEMBERS

William F. Thomas, Director, Readiness and Operational Support Directorate
Harrell D. Spoons, Program Director
Marvin L. Peek, Project Manager
John Van Horn, Team Leader
Adrienne Brown, Team Leader
Steve Borushko, Auditor
Lynn Concepcion, Auditor
Lisa Earp, Auditor
Rhonda Carter, Auditor
Nancy C. Cipolla, Editor
Paula D. Stark, Secretary

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 99 1999



TAB 3

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 100 1999



Monday, June 20, 1994

Robert J. Lieberman
Assistant Inspector General
for Auditing
Department of Defense
400 Army Navy Drive
Arlington, Virginia 22202-2884

Re: Audit Report on Controls Over Copyrighted Computer Software (Report No. 93-056)

Software Publishers Association

Dear Assistant Inspector General Lieberman:

The Software Publishers Association (SPA) is the primary trade association representing the software industry, with over 1100 members. Our mandate is to promote and defend our members' intellectual property rights. Under this mandate, we seek to educate the public about intellectual property rights related to software, to assist the public in complying with the copyright laws, and to enforce our members rights via audits and, if necessary, litigation. Enclosed is some general information concerning the SPA and our activities.

This letter is to inquire about the status of the recommendations and/or follow-up concerning your audit for unauthorized software on the Department of Defenses' computers in February 1993. We have a copy of Report No. 93-056. The information in the report caused great concern to the SPA. If the report was accurate in its estimate that 51% of the tested computers contain unauthorized software, extrapolated to the total computers within the Department of Defense, the level of infringement is significant. We recognize that 16 months have passed and that this situation may have been addressed since issuance of this report. We therefore would appreciate receiving any follow-up reports, recommendations or other information concerning the Department of Defense's compliance with the federal copyright laws.

We would be pleased to work with you to bring the Department of Defense into compliance with the federal copyrights laws and to establish an effective education and maintenance program. To this end, we can provide advice, educational materials, and conduct classes or lectures for the Department of Defense. I would be happy to discuss further the assistance we can provide.

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 101 1999

I would appreciate receiving any follow-up reports, recommendations, directives, etc. by June 30, 1994. Please feel free to call me at 202-452-1600 x. 311 with any questions. I look forward to talking to you soon.

Sincerely,

/s/

Sandra A. Sellers
Director of Litigation

Encl.

Software Publishers Association

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 102 1999

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

OCT 17 1994

Ms. Sandra A. Sellert
Director of Litigation
Software Publishers Association
1730 M Street NW, Suite 700
Washington, D.C. 20036-4510

Dear Ms. Sellert:

This is in reply to your letter of June 20, 1994 regarding this office's February 1993 report on the use of unauthorized software by Department of Defense employees. As indicated in that report, management reaction to the draft was mixed. However, responses to the final report were more positive and the Department is taking measures to increase the awareness of its employees to applicable copyright considerations and to improve internal controls. A copy of September 1993 guidance issued by the Secretary of Defense is enclosed. A comprehensive software management directive is due out in draft in July 1994. We do not have any current information on what measures the individual military departments and agencies are taking, but the topic will be considered for a followup audit during the next couple years.

We appreciate your offer of assistance on this matter. In this Department, however, providing the requisite training is primarily a management function. Therefore we suggest you may wish to contact the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) or individual component heads.

We share your concern about this problem and are pleased that you found our report useful.

Sincerely,

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Enclosure

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 103 1999

ASSISTANT SECRETARY OF DEFENSE
WASHINGTON D C 20301-3040

COMMAND, CONTROL
COMMUNICATIONS
AND
INTELLIGENCE

September 27, 1993

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
COMPTROLLER
GENERAL COUNSEL
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Computer Software Copyright Protection

On February 19, 1993, the DoD Inspector General published an Audit Report entitled "Controls Over Copyrighted Computer Software," (Report No. 93-056), which found that there were a significant number of software programs installed on DoD computers that cannot be shown to have been purchased. I want to emphasize existing Departmental policy prohibiting the unauthorized use and copying of commercial software programs.

Vendors should not be deprived of their legitimate revenues through unauthorized use of their proprietary software. We must ensure that DoD employees do not copy or use unauthorized software programs.

It is my desire that the ethical behavior of Department of Defense employees, both military, and civilian, be a positive example to all of Government.

Emmett Paige, Jr.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 104 1999



Wednesday, August 10, 1994

Robert J. Lieberman
Assistant Inspector General
for Auditing
Department of Defense
400 Army Navy Drive
Arlington, Virginia 22202-2884

Re: Audit Report on Controls Over Copyrighted Computer Software (Report No. 93-056)

Software
Publishers
Association

Dear Assistant Inspector General Lieberman:

This is further to your letter of June 27, and my letter of June 20, 1994, concerning your office's report on the use of unauthorized software by the Department of Defense. In your letter of June 27, you indicated that a comprehensive software management directive was due out in draft in July 1994. Would you please send me a copy of that directive? Thank you for sharing our concern about the necessity of software management and the protection of U.S. copyrights granted to our members.

Sincerely,

Sandra A. Sellers

Sandra A. Sellers
Director of Litigation

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 105 1999

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON VIRGINIA 22202 2884

Analysis
and Followup

AUG 25 1994

Ms. Sandra A. Sellers
Director of Litigation
Software Publishers Association
1730 M Street NW, Suite 700
Washington, D.C. 20036-4510

Re: "Audit Report on Controls Over Copyrighted Computer Software" (Report No. 93-050)

Dear Ms. Sellers:

This is in reply to your letter of August 10, 1994, to Mr. Robert J. Lieberman requesting a copy of the Department of Defense draft guidance for software management. My office tracks agreed-upon actions on audit recommendations, and we are monitoring the status of the directive you requested.

The directive is being readied for formal coordination with the Department of Defense Components, a required process prior to issuance of DoD policy guidance. In checking its current status, we were advised that the following language is planned for inclusion in the proposed directive:

> "Contractual terms and conditions for use of software, including copyright and license agreements, shall be carefully followed and strictly enforced."

We understand that in January 1995 the guidance will be approved, published and available for external distribution. At that time, you may wish to request a copy of the directive from the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (telephone number 703-695-0348), the proponent of the directive. Of course, my office will continue to monitor the issuance of this guidance under our normal followup procedures.

David A. Brinkman
Assistant Inspector General

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 106 1999



31 May 1995

Ms. Nadine K. Dulacki
Chief
FOIA Office
Room 4A5A
Department of Defense
400 Army Navy Drive
Arlington, VA 22202-2884

Software Publishers Association

Dear Ms. Dulacki:

I recently wrote to your office requesting a copy of Audit Report 93-05e "Controls over Copyrighted Computer Software," dated February 19, 1993. In fact, we already have this report, but it is the follow-up directive which we would like to receive.

I have attached a letter from David Brinkman, Assistant Inspector General, dated 25 August 1994 and addressed to my boss, Sandra Sellers, Director of Litigation. Mr. Brinkman's letter addresses the directive I am requesting, explaining that the directive was supposed to be issued and published in January 1995. I am attaching Mr. Brinkman's letter for the sake of clarity, since my previous request was for the wrong document.

Please let me know if there are fees associated with my request, and I will arrange for payment. I appreciate your assistance in this matter, and I look forward to receiving the directive at your earliest convenience.

Sincerely,

Christine Keck
International Coordinator

Enclosure

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 107 1999

OFFICE OF THE ASSISTANT TO THE SECRETARY OF DEFENSE
1400 DEFENSE PENTAGON
WASHINGTON D C 20301 1400

PUBLIC AFFAIRS

31 JUL 1995

Ref: 95-F-1119

Ms. Christine Keck
Software Publishers Association
1730 M Street, Suite 700
Washington, DC 20036-4510

Dear Ms. Keck:

This responds to your Freedom of Information Act (FOIA) request of May 31 1995, to the Office of the Department of Defense Inspector General (DoDIG). Your request was received in this Directorate on June 16, 1995. Our interim response of June 21, 1995, refers.

The Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD C3I) has provided the following comments concerning DoD Directive 3405.1 - Software Management).

"The requested directive (DoD Directive 3405.1 - Software Management) was not signed and published in January 1995 as originally targeted. The directive has gone through a major rewrite due in part to the Department's objective of streamlining policy documents and the need to incorporate additional software policy language published by ASD(C3I) memos and Defense Science Board recommendations. The current draft document has not been formally staffed within the Department and, therefore, no formal Department policy position has been reached."

Consequently, Mr. William K. O'Donnell, an Initial Denial Authority for the OASD(C3I), has denied release of the document under the provisions of 5 U.S.C. 552 (b)(5). You may appeal Mr. O'Donnell's decision by offering justification to support reversal of the initial denial. Any such appeal should be forwarded within 60 calendar days of the date above to the Office of the Assistant to the Secretary of Defense for Public Affairs, Directorate for Freedom of Information and Security Review, Room 2C757, 1400 Defense Pentagon, Washington, D.C. 20301-1400.

The OASD(C3I) also stated that the document is scheduled to be signed by the Deputy Secretary of Defense, and available for public release by December 1995. Current plans include making the document available on the ASD(C3I) World Wide Web Homepage. Additionally, most DoD Directives are available to the public outside of FOIA channels from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22151.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 108 1999

There are no assessable fees for this response in this instance.

Sincerely,

A. H. Passarella
Director
Freedom of Information and
Security Review

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 109 1999

TAB 4

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 110 1999



August 9, 1996

Via Overnight Mail

Ms. Katherine Knittel
Dept. of Labor, Mine Safety and Health Administration
730 Simms Street
Lakewood, CO 80401

Dear Ms. Knittel

I am writing on behalf of the Software Publishers Association (SPA), which is the principal trade group of the PC software industry. Many of our more than 1,500 member companies look to the SPA to help stop the unauthorized duplication of their products. We are writing this letter on behalf of the SPA members set forth as Exhibit A attached hereto.

Software Publishers Association

We have received information that Dept. of Labor, Mine Safety and Health Administration may be using unauthorized copies of our members' software in violation of Federal copyright law. From the information we have obtained, the software involved is published by SPA members listed on Exhibit A attached hereto.

We hope this unauthorized duplication does not reflect official policy for your company. Under the circumstances, however, we would like to suggest an audit of your company as an alternative to litigation. The procedure for the SPA audit program is as follows:

1. An SPA representative observes as the software directories of each PC are printed.
2. Directory information is compared with purchase records to determine the number of unauthorized copies, if any;
3. You destroy all unauthorized copies, and agree to use only authorized software in your business;
4. You agree to pay the SPA Copyright Protection Fund an amount equal to the manufacturer suggested retail price of any unauthorized software, and
5. If necessary, SPA executes a release from liability for infringement discovered.

As you will note from the enclosed articles, the SPA has an active litigation program. We are at this time providing your organization the opportunity to bring itself into compliance with the Federal copyright laws without litigation. We caution you not to destroy any software prior to the resolution of this matter, as the destruction of material evidence may give rise to additional liability.

I would appreciate your contacting me as soon as possible, and in any event no later than Tuesday, August 13, 1996. If I am not available, please ask to speak to Joshua Bauchner at extension 323.

Sincerely,

Peter Beruk
Director of Domestic Anti-Piracy

enclosures

1730 M Street • Suite 700 • Washington, DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 111 1999

U. S. Department of Labor

Mine Safety and Health Administration
P.O. Box 25367
Denver, Colorado 80225-0367

August 13, 1996

Mr. Peter Beruk
Director of Domestic Anti-Piracy
Software Publishers Association
1730 M Street, Suite 700
Washington, DC 20036-4510

Dear Mr. Beruk:

This is in response to the package we received yesterday from your organization concerning allegations of possible use of unauthorized copies of software published by members of your organization. Contrary to the apparent assumptions in your threatening form letter, we are not a private company or organization, but a federal government agency in the United States Department of Labor. Moreover, I can assure you that it is not the policy of the Mine Safety and Health Administration (MSHA) to use unauthorized or pirated software, and that we make every effort to ensure that all software copies are covered by appropriate licensing agreements.

We would appreciate any information you could provide concerning these serious allegations and your threat of suit, e.g. which software you believe is being used improperly, and where in this nation-wide organization that abuse is occurring. I would be happy to discuss any real concerns you might have, but not without some concrete evidence to support your allegations and to give me a basis for investigation. In addition, I am not able nor willing to authorize you or your organization to have access to any of our government applications or software directories on the basis of your conclusory and threatening letter.

I have shared your letter with the Office of the Solicitor, Department of Labor and with MSHA's National Headquarters in Arlington, Virginia, in order to get further guidance in preparing this response.

Sincerely,

Kathrine L. Knittel
Chief, Information Resource Center

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 112 1999

August 19, 1996

Via Overnight Mail and
Facsimile: 303-231-5447

Ms. Katherine Knittel
US Department of Labor
Mine Safety and Health Administration
730 Simms Street
Lakewood, CO 80401

Dear Ms. Knittel,

Software Publishers Association

Thank you for your letter dated August 13, 1996. Pursuant to our conversation on August 16, I would like to take this opportunity to address some of the questions you raised.

SPA received a report that your organization was using unauthorized copies of our members software at the Lakewood, Colorado and Arlington, Virginia sites. Upon receipt of this information, SPA conducted a preliminary investigation and determined that a cooperative audit was the best way to effectively resolve this matter. (The audit steps are detailed in the August 9, 1996 letter to you from Peter Beruk.)

According to our information a significant amount of software is unauthorized. These titles include, but are not limited to, AfterDark, PC Tools, WordPerfect, Norton Utilities, and others.

In light of the above, SPA would like to conduct a cooperative audit, on behalf of its member companies, with the US Department of Labor, Mine Safety and Health Administration. A copy of the standard audit agreement will follow by mail.

Please call me at your earliest convenience to discuss proceeding with this process. I may be reached at 202-452-1600 extension 322. Thank you for your cooperation.

Sincerely,

Joshua Bauchner
Litigation Coordinator

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 113 1999

U.S. Department of Labor

Mine Safety and Health Administration
4015 Wilson Boulevard
Arlington, Virginia 22203-1984

18 SEP 1995

Mr. Joshua Bauchner
Litigation Coordinator
Software Publishers Association
1730 M Street, Suite 700
Washington, D.C. 20036-4510

Dear Mr. Bauchner:

This is in response to your recent correspondence to Ms. Kathrine Knittel, who is on my staff in Lakewood, Colorado, concerning allegations of unauthorized use of software within the Mine Safety and Health Administration (MSHA), particularly at our locations in Arlington, Virginia, and Lakewood, Colorado.

I have reviewed the audit agreement that you included with your last correspondence to Ms. Knittel, and discussed it with our Solicitor's Office. Based on their counsel, I must inform you that I have no authority to enter into this type of agreement, which you apparently use with private companies, or to bind the Agency to pay the monetary penalties stipulated. For further information on this issue, you may contact Thomas A. Mascolino, Deputy Associate Solicitor for Mine Safety and Health, at (703) 235-1155.

As a Federal regulatory Agency, our primary mission and responsibility is to protect the safety and health of the Nation's miners, while making the best use possible of the resources provided to us by the American taxpayer. The audit you are proposing would make an enormous, unreasonable and unjustifiable drain on these resources, at a time when resources are tight, and getting tighter. Further, from the preliminary information that I have been provided, I do not believe that the problem you are alleging is of sufficient scope to warrant such an investment of time and resources.

A quick review of our records indicates that MSHA has acquired through Softmart, Incorporated, sufficient upgrade licenses for 289 simultaneous users of WordPerfect for Windows, Version 6.1. The 289 licenses for WordPerfect 5.1 that were used as the basis of this upgrade were acquired through a contract between the U.S. Department of Labor and WordPerfect Corporation. A significant number of these licenses have been assigned to file servers in Lakewood, Colorado, and Arlington, Virginia, where they have been

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 114 1999

metered. Accordingly, it is quite difficult to believe that MSHA could be in violation of our WordPerfect licensing agreements. Also, while our research is far from complete, we have found a single acquisition of 166 copies of Norton Utilities through Egghead Discount Software. While research is continuing with respect to the other software products that you referenced, I do not believe that copyright violations are rampant in MSHA. Based on these findings, I would suggest that you re-examine the validity of the information you have been provided.

Notwithstanding the above, I am concerned that the Agency re-address its policies and practices in regard to software management. Accordingly, I have asked Ms. Knittel and her staff to develop a management plan to address this issue and to provide me and the Agency with the best assurance possible that we are adhering to all applicable software licensing agreements and copyright laws.

I can be reached at (703) 235-8378, if you wish to discuss this matter further.

Sincerely,

George M. Fesak

George M. Fesak
Director, Program Evaluation
and Information Resources

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 115 1999



December 10, 1996

Via Overnight Mail

Charles C Masten
Inspector General
Department of Labor
200 Constitution Avenue, Room S1303
Washington, DC 20004

Re: Proposed Audit of Mine Safety and Health Administration

Dear Inspector General Masten

Software Publishers Association

I am writing on behalf of the Software Publishers Association (SPA), which is the principal trade group of the PC software industry We have authorization from those members listed on Exhibit A, attached hereto, to investigate allegations of copyright infringement of their products

On August 9, 1996, SPA contacted the Department of Labor's Mine Safety and Health Administration office in Lakewood, Colorado We had received information that the unauthorized duplication of our members' software was occurring within the Administration at this and other sites. Ms Katherine Knittel, of the Lakewood office, directed our investigators to contact Mr George Fesak at the Arlington, Virginia office

After lengthy discussions, Mr Fesak has indicated that he has been unable to receive the necessary authorization to conduct a cooperative audit with SPA of the software installed on MSHA's computers Mr. Fesak has indicated that violations may exist, as does the need for an audit However, without the necessary approval, he is unable to proceed

As I am sure you are aware, copyright infringement is a serious matter and warrants immediate investigation and remedy Title 17 of the United States Code provides for significant damages to be awarded to copyright holders for unauthorized use of their product The Federal government is, of course, not exempt

It is SPA's intention to work cooperatively with MSHA to resolve this matter We conduct over 500 actions each year, 90% of which are resolved via the audit process Please find enclosed the original audit letter, Exhibit A, and copies of all correspondence to date Upon review of the material, I would appreciate your contacting me to discuss how we may resolve this situation I may be reached at 202-452-1600 extension 311 If I am unavailable, please contact Joshua Bauchner at extension 323 Thank you for your kind attention to this matter

Sincerely,

Sandra Sellers
Vice President Intellectual Property
Education and Enforcement

enclosures

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452 1600 • Fax (202) 223 8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 116 1999

Date. January 10, 1997

To: George Fesak, Keith Galayda, Shirley Malia, Department of Labor

From: Sandra Sellers, Joshua Bauchner, Software Publishers Association

Re: Cooperative Efforts Between DOL and SPA

As a result of our meeting on January 8, 1997, we would like to detail some of the elements to which we agreed. In general, these are twofold: a software audit of MSHA and the implementation of educational and procedural measures throughout the DOL as a whole.

MSHA Audit

As a result of specific allegations having been made against MSHA, it was decided that a comprehensive software audit was to be conducted over approximately 10 months time Mr Fesak was to determine an appropriate schedule for the audit and provide it to SPA. The results of the audit are to be provided to SPA via the Inspector General's office. SPA requested five specific terms for completion of the audit:

1. maintain a schedule
2. provide a summary of all software found
3. provide a summary of all documentation found to substantiate the legality of software
4. provide a final report of all infringing software destroyed and/or purchased to ensure legality
5. develop and implement measures to ensure future compliance

As mentioned at the meeting, SPA is willing to provide assistance in conducting the audit. Mr Bauchner will be available to answer any and all questions arising during the audit process and to receive the reports as they become available.

DOL Software Education and Policy

At a department level, it was agreed that DOL would implement procedures and policies to heighten awareness and maintain compliance. Suggested policies include, but are not limited to a software use policy, an employee code of ethics pertaining to software, a software acquisition policy, and an audit policy.

SPA agreed to forward copies of its suggested software use policies for review by DOL. Please find them attached SPA has also provided to Mr. Fesak and Ms. Malia copies of its Certified Software Management course manual. The manual includes these policies as well as additional information vital to ensuring legal software use.

Upon receipt of the above material, DOL will provide to SPA a copy of its draft *Appropriate Use Document* for review It is SPA's intention to work cooperatively with DOL to develop and implement the appropriate policies and awareness programs to promote software compliance As such, SPA is willing to offer to DOL any resources available including: posters, policy statements, anti-piracy presentations, the CSM course, and any other requested material or information.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 117 1999

January 10, 1997

To: Sandra Seller and Joshua Bauchner, Software Publishers Association

From: Keith E. Galayda, Office of Inspector General, Audit, Assistant Director

Subject: SPA's Summary of January 8, 1997 Meeting

The discussions held that day between MSHA, DOL, OIG, and SPA should be characterized a little different, I believe. I rather we project the cooperative nature of the meeting, which it was, and the need to do things better regarding the protection of intellectual property. The actions of MSHA and the Department with the OIG providing oversight should go a long way in raising the awareness of software copyright laws. SPA should acknowledge these Government officials have pledged to address this issue of awareness through implementing:

- better software education and policy,
- better software documentation management, and
- periodic accountability reviews (one completed within 9 mo - 1 yr)

The OIG, through auditing this issue over the past 5 years, believes awareness is the problem and must be reinforced. As acknowledged in your summary of the meeting, the various parties are willing to assist each other in addressing this issue, even though the allegations received are unsubstantiated. As I stressed, the importance of our addressing this issue is not to substantiate specific allegations but to move beyond any allegations so that adequate controls can be ensured and awareness can be heightened.

OIG will have a role in ensuring the "pledge of action" will not be left unaddressed and everyone involved can be satisfied with the results of our commitments. OIG will communicate the results of the Government's actions to SPA has they are completed or become finalized.

I believe we all are trying to do the right thing here and I want to thank SPA for the assistance offered in providing relevant materials. As suggested, all parties would meet sometime in the future to discuss our actions and accomplishments.

cc: George Fesak
Shirley Malia

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 118 1999



U.S. DEPARTMENT OF LABOR
OFFICE OF INSPECTOR GENERAL
OFFICE OF PERFORMANCE AUDITS

FAX TRANSMISSION

TO: SANDRA SELLERS / JOSH DAUCHNER

Fax No. ( ) 223-8756 **Telephone No. (**)_____

From: KEITH GALAYDA

_____

Fax No. (202) 219-4865 Telephone No. ( )_____

_____ **page(s) follow**

COMMENTS _____

_____

_____

_____

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 119 1999

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

FEB 5 1997

Software Publishers Association
1730 M Street, N.W.
Suite 700
Washington, D.C. 20036

Dear Mr. Joshua Bauchner and Ms. Sandra Sellers:

Enclosed is a draft copy of the Department of Labor's policy on Appropriate Use of Microcomputers and LANs. A copy of this draft has been sent also to the Office of the Inspector General, the Mine Safety and Health Administration and the Department's Labor Relations Office for sharing with the Department's two union partners, as required by contract with them

The respective Collective Bargaining Agreements, by law, provide for each union (the National Council of Field Labor Locals (NCFLL) and the Local 12, American Federation of Government Employees, AFL-CIO) to request, if desired, bargaining over any changes to conditions of employment or impact and implementation bargaining on decision exercised by management The Agreements provide a process for each union to respond to management proposals We anticipate hearing from each union in the very near future. At that time, we will conduct the necessary negotiations, if any, and advise you of our implemenation plans.

The policy was previously reviewed by all DOL agencies representatives, and is ready for implementation upon union approval. It includes statements on Internet usage, software licensing and usage, shareware licensing, and all other areas of concern expressed by you as representatives of Software Publishers Association in our January 9, 1997 meeting.

We thank you for your willingness to share your concerns and suggested policy statements with us. Both have been beneficial

Sincerely,

Shirley A. Malia
Director
Information Technology Center

Enclosure

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 120 1999

DLMS 9 - INFORMATION TECHNOLOGY

Chapter 1200 - MICROCOMPUTER AND LAN MANAGEMENT

Paragraph	Contents	Page
1200	MICROCOMPUTER AND LAN MANAGEMENT	12-1
1201	Purpose	12-1
1202	Background	12-1
1203	Authorities	12-1
1204	Policy	12-1
1205	Scope	12-1
1206	Responsibilities	12-1
1206a	Chief Information Officer	12-1
1206b	The Director, Information Technology Center	12-1
1206c	DOL Agency Heads	12-2
1207	Microcomputer LAN Management, Operational and Security Requirements	12-2
1207a	LAN Administration	12-2
1207b	Physical Security and Access Controls	12-3
1207c	Password Protection	12-4
1207d	Virus Protection	12-4
1207e	Backup and Offsite Storage of LAN Information Resources	12-4
1207f	Offsite Use of Government-Owned Equipment	12-4
1207g	Copyright Licensing Requirements	12-5
1207h	LAN Interconnectivity	12-5
1208	Appropriate Use of DOL Information Technology	12-5
1208a	Purpose	12-5
1208b	Notice of Auditing/Monitoring	12-5
1208c	Personal Use	12-6
1208d	Responsible Users	12-6
1208e	Restrictions	12-6
1208f	Penalties	12-7
1208g	Internet Use	12-7

Appendix A-1207, ADP Security Certification, U.S. Department of Labor Contract Personnel 12-8

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 121 1999

1200 Microcomputer and LAN Management

1201 Purpose. This chapter establishes policy guidance, responsibilities for the management, security and the appropriate use of microcomputer based Local Area Network (LAN) information resources.

1202 Background. Each Department of Labor (DOL) Agency is responsible for determining the level of security for each LAN based on an assessment of information being processed. When the information processed and stored on a LAN is sensitive or critical to the mission of the Agency, the level of security must be consistent with DLMS 9, Chapter 500.

1203 Authorities. Computer Fraud and Abuse Act of 1986 (Public Law 99-474.); Computer Security Act of 1987 (Public Law 100-235); Freedom of Information Act; Paperwork Reduction Act of 1995; Information Technology Management Reform Act of 1996; Management of Federal Information Resources (Office of Management and Budget Circular No.A-130); and the Federal Information Processing Standards (FIPS).

1204 Policy. Reasonable operational and security measures are required to safeguard microcomputer, LAN, telecommunication, and peripheral information resources. DOL Agencies should protect their information technology investment with physical security and affordable contingency planning (see 1207, below).

Government owned microcomputers and other information technology resources are to be used for official business purposes, including use by union officials for appropriate labor-management relations activity. However, DOL permits employees to use government computers during non-work time for limited personal use, and within established guidelines (see 1208, below).

1205 Scope. This chapter applies to all DOL microcomputer and LAN systems. The primary objective in formulating microcomputer and LAN management policy is to provide guidance to DOL Agencies in implementing a program which ensures regulatory and standards compliance as well as effective management and operation of microcomputer and LAN systems.

1206 Responsibilities. In addition to the responsibilities set forth in DLMS 9 Chapter 500, "Security" this paragraph establishes specific microcomputer-based LAN management and security responsibilities.

a. The Chief Information Officer (CIO) is responsible for:

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 122 1999

(1) Establishing LAN interconnectivity standards to ensure functionality across DOL LANs.

(2) Conducting or delegating to Agency Heads the performance of information resources management reviews of each microcomputer and LAN management practices to ensure compliance with accepted standards and this chapter (see: Paperwork Reduction Act of 1995).

b. The Director, Information Technology Center (ITC), OASAM is responsible for:

(1) Maintaining the Employee Computer Network (ECN), including establishing standards and conventions for ECN users.

(2) Establishing configuration requirements for LANs used to develop and maintain administrative systems (e.g., DOLAR and PERMIS), in conjunction with the Office of the Chief Financial Officer, and other subject matter authorities.

c. DOL Agency Heads are responsible for:

(1) Determining the level of sensitivity, analyzing risks/exposures, and developing appropriate safeguards for IT investments.

(2) Adequately maintaining and securing agency-dedicated microcomputer and LAN information resources.

(3) Ensuring that LAN managers/administrators and end-users receive necessary instruction for the management, security, and use of microcomputer and LAN information resources.

(4) Ensuring that sensitive information is safeguarded while in the microcomputer/LAN environment. The security plan governing such information must follow guidelines in DLMS 9, Chapter 500.

(5) Complying with LAN interconnectivity standards and review schedules established by the CIO.

(6) Ensuring that software placed on agency PCS/LANs is licensed, and employees are made aware of licensing requirements.

1207 Microcomputer LAN Management, Operational and Security Requirements.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 123 1999

a. LAN Administration: Recognizing the unique characteristics of microcomputers and LANs as distributed computer systems with decentralized processing capabilities, agencies shall identify and train a specific person s to function as a LAN Administrator as well as a backup Administrat for each Agency LAN. In addition, Agencies should maintain written documentation which includes the LAN configuration, operational procedures, and standards.

b. Physical Security and Access Controls. Each Agency sha ensure that FIP resources are operated and maintained to safeguard the confidentiality, integrity, and availability of information, including prevention of loss from natural hazards, fire, and accidents.

Also, Agencies shall maintain a user profile which indicates all access privileges users have through direct or remote LAN connectivity as well as accessibility to external data systems (i.e., Data Resources Inc., Dow Jones, Wall Street Journal, Mead Data Central, etc.).

In addition to ensuring adequate physical security of LANs, Agencies should develop procedures that include the following:

(1) Establishing end-user accountability for computer use and requiring that proper security procedures be observed by employees.

(2) Granting employee access to information technology resources based upon job-related need.

(3) Restricting access to sensitive information through encrypted and/or password protected text and data files. Alternatively, sensitive information, can be confined to limited access areas on the LAN file server or can be maintained on removable storage media, and locked up, as appropriate, when not in use. Sensitive information should not reside on the local PC hard disk, unless it is protected.

(4) Erasing or removing a hard disk to remove all information before designating equipment as surplus.

(5) Protecting information stored on a microcomputer or LAN server from being tampered with.

(6) Ensure completion of Separation Clearance Form DL 1-107, Section 1, for departing federal employees or ADP Certification Form for Contract Personnel for departing contract

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 124 1999

personnel. (See Appendix A 1207.)

c. Password Protection. Since PCS LANs provide gateway access into various interconnected, mission critical automated information systems, passwords are an essential line of defense to deter unauthorized intrusion and maintain a proper level of LAN security. Therefore, agencies should develop and enforce a password system based on the degree of protection warranted by the sensitivity of the system and the data.

d. Virus Protection. Effective virus protection strategies must integrate practices which span all areas of computer security, including issues relative to physical/installation security, access controls, disk scanning, software testing and installation, backup and recovery, use of up-to-date virus detection tools, and user education/training. To ensure effective virus protection, Agencies should as a minimum:

(1) Implement an action plan to deal with potential incidents.

(2) Scan network PCS on a regular basis.

(3) Perform software scanning periodically on stand-alone PCS.

(4) Prohibit the use of software and data files that have not been authorized by the Agency and scanned for viruses.

(5) Educate employees to the need for virus awareness and prevention.

e. Backup and Offsite Storage of LAN Information Resources. Backup and offsite storage of computer application and data files will ensure that Agencies have recent copies available in case of loss of working copies. Off-the-shelf and applications software developed or maintained locally should also be backed up. Source program files, executable versions of all software, and required compiler or interpreter programs should be included as well. Accordingly, to ensure the safety and availability of all data and program files produced, Agencies shall:

(1) Provide instruction to employees for backup of data.

(2) Safekeep vital files at an off-site facility, as necessary, to protect against threats or sabotage.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 125 1999

f. Offsite Use of Government-Owned Equipment. The use of Government-owned computer equipment carries with it an obligation to be accountable for the security of the equipment and for how it is used. To foster the protection of the Government's interest and computer assets, DOL Agencies should develop procedures that:

(1) Restrict the removal of sensitive data from the worksite unless cleared by the immediate supervisor.

(2) Provide instructions to employees concerning physical and data security, as well as hardware, software, operational and maintenance procedures prior to approval or release of equipment from DOL premises.

g. Copyright/Licensing Requirements. Most commercial software is protected by copyright law. Some packages may also be patented, which gives them added protection. When an organization "purchases" a commercial software package, it usually only purchases the right (the "license") to use the package in a manner deemed appropriate by the owner. The ownership of the "intellectual property," the underlying program code, usually remains with the author or publisher. Therefore, pursuant to the law and regulation governing software licensing, DOL Agencies shall develop internal procedures to ensure that all microcomputer/LAN users comply with existing statutes, regulations and license agreements governing the use and disposition of proprietary software including shareware. As a minimum, such procedures will include designation of a software manager, recordation of the number of purchased licences by software product, recordation of distribution, and periodic auditing of product usage.

h. LAN Interconnectivity. Agencies shall comply with standards designed to ensure LAN interconnectivity for administrative systems compatibility, executive and inter-agency communications.

1208 Appropriate Use of DOL Information Technology.

a. Purpose: Computer-based information, recognized as a primary government asset, should be protected from unauthorized modification, destruction, disruption, or disclosure--whether accidental or intentional.

b. Notice of Auditing/Monitoring: Users must be advised that they have no expectation of privacy while using any government owned or leased system, which includes workstations,

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 126 1999

LAN servers, and all software such as word processors, Internet browsers, electronic mail, etc. Activity on Department of Labor information technology systems and equipment is subject to FOIA requests, to monitoring in the course of systems administration, and to audit or law enforcement reviews to protect the system from inappropriate use. Unauthorized use of this system is a violation of Federal law and can be punished with fines or imprisonments (P. L. 99-474). Anyone using this system expressly consents to such monitoring, and violations may be reported to the proper authorities.

c. Personal Use: DOL's automation systems have been established for the purpose of conducting official Agency business. However, the Department recognizes that frequent use of a microcomputer enhances the skill of the user. Therefore, responsible employees are authorized to use DOL microcomputers during non-working hours for personal use, subject to limitations defined in d. and e. below.

d. Responsible Users: Responsible staff personal use would entail:

(1) The ethics and conduct requirements for Department of Labor employees set forth at 5 C.F.R. Part 2635 shall apply to all Labor Department employees in their use of Department microcomputers.

(2 Use fully complies with general agency policy regarding limitations on uses of DOL information technology;

(3) Use occurs during the employee's personal time;

(4) Use does not incur any additional direct charges, such as services which are charged on a time or usage basis;

(5) Requesting supervisory approval for described activity.

e. Restrictions: Department of Labor employees are prohibited from the following uses of DOL microcomputers, unless specifically authorized by the agency:

(1) Interfering with the conduct of official agency business;

(2) Engaging in political activities that are forbidden by federal rules, such as the Hatch Act;

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 127 1999

(3) Accessing material that would not be suitable for public distribution in worksites, such as obscene materials;

(4) Using commercial subscription services;

(5) Game playing or gambling;

(6) Using Internet access for data or discussions that would cause the Department embarrassment;

(7) Engaging in private, for profit business activity, performing computing services for commercial purposes, or using any DOL computer resource including DOL software for personal profit or personal gain;

(8) Possessing, installing, or using programs capable of fraudulently simulating systems responses;

(9) Possessing, installing, or using programs that erase or alter files maliciously or without authorization;

(10) Loading undelivered or personal software;

(11) Modifying or possessing systems control information, especially that which affects program state, status, or accounting, maliciously or without authorization;

(12) Interfering with systems efficiency or attempting to modify or crash the system;

(13) Using another person's name and password, or accessing unauthorized files.

f. Penalties: Violations of this policy, unauthorized or inappropriate use or abuse of DOL information resources may be subject to disciplinary action and legal sanctions.

g. Internet Use: The Department of Labor encourages its employees to use the Internet to accomplish job responsibilities and furtner mission goals. Excessive use, or "surfing the Internet" during working hours is prohibited.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 128 1999

Date Apnl 9, 1997

To Keith Galayda, Department of Labor

From Sandra Sellers, Joshua Bauchner, Software Publishers Association

Re Cooperative Efforts Between DOL and SPA

As a result of our conference call on Apnl 8, 1997, we would like to summarize DOL's representations regarding the establishment of policies and procedures to ensure software compliance within the Department as a whole and the Mine Safety and Health Administration

Software Publishers Association

Pursuant to our earlier memo dated January 10, 1997, SPA's interests are twofold First, we request that a software audit be conducted and concluded within MSHA by the third or fourth quarter of this calendar year Second, SPA seeks to cooperate with DOL as a whole to develop and implement software policies and procedures

As such, Mr. Galayda stipulated during our phone conversation on April 8, that DOL currently had a software policy in the final stages of development He indicated that the policy awaited union approval and that he expected the entire process to be completed within the month

Similarly, within MSHA, Mr Galayda stated that a software policy was being drafted by Mr George Fesak at MSHA The draft policy has been viewed by Mr Galayda and will be subject to his approval Included in the effort is a three step process to ensure software compliance

1. develop and implement a software policy and establish controls
2. assign accountability and train appropriate personnel
3. conduct accountability reviews (audits)

According to Mr Galayda, the MSHA policy will be implemented after the Department wide policy as it is intended to complement that policy In addition, he indicated that the MSHA software policy will be completed within the month

While that policy is being reviewed and approved, MSHA would begin to assign accountability and arrange training, which would be ready for implementation by the time the policy is approved It would then take little time to actually conduct the accountability reviews, so we will be on track for completing the entire process, including the audit of MSHA

Finally, Mr Galayda agreed with SPA's continued request that the three step MSHA effort, as defined above, be completed by the third or fourth quarter of this calendar year, as is consistent with the schedule set forth at the January 10th meeting

1730 M Street • Suite 700 • Washington DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 129 1999

U.S. Department of Labor

May 27, 1997

Ms. Sandra Sellers
Vice President, Intellectual Property
Software Publishers Association
1730 M Street NW, Suite 700
Washington, DC 20036-4510

Dear Ms. Sellers:

As promised during our meeting on January 8, 1997, we have developed a plan for enhancing software management within the Mine Safety and Health Administration (MSHA). In preparing this plan, we consulted with officials in the Department of Labor's Information Technology Center and Office of the Inspector General.

The primary components of our plan, with projected completion dates, are as follows.

1. We will issue Agency-wide policy letters on the Internet and software licensing and management. The Internet policy letter will provide policy guidance for MSHA employees in the appropriate use of the Internet. The software licensing and management policy letter will establish MSHA policy for software management, document the legal obligations inherent in the purchase and use of computer software, and inform Agency employees of their responsibility for complying with software license agreements. Both policy letters are currently in the review process. We expect to issue the policies by July 1997. A copy of each draft policy letter is enclosed for your information.

2. We will establish and staff a software coordinator position within the Information Resource Center in Lakewood, Colorado. While software is used in every office of the Agency throughout the nation, we believe it is essential that software licensing be centrally managed. We plan to have the software coordinator position established and filled by July 1, 1997.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 130 1999

3. We will procure a software management tool, establish specific procedures for tracking and managing software licenses, and issue an Administrative Information Bulletin to inform all MSHA employees of those procedures. We will complete these tasks by September 1, 1997.

4. We will review procurement records to assess current software license status. The information from this review will provide the initial data to load the software management tool discussed in Item 3. The review will be completed by October 15, 1997.

5. We will conduct a software audit in Arlington, Virginia, and Lakewood, Colorado. Included in the audit will be the LAN servers, all LAN work stations, and all laptop and stand-alone computers assigned to personnel in Arlington and Lakewood. As part of the audit process, we will produce a final report documenting the audit findings and furnish this report to the Office of the Inspector General. The audit will be completed by December 30, 1997.

I believe that implementation of this plan will ensure that MSHA is complying with applicable software licensing laws and will raise the awareness on the part of Agency managers and employees of their responsibilities for complying with those laws.

I appreciate your assistance in bringing this issue to our attention and providing us with guidelines and background materials on software management. If you have any questions or comments about our plan, please contact Keith Galayda of the Office of the Inspector General. Mr. Galayda can be reached on (202) 219-6641.

Sincerely,

George M. Fesak

George M. Fesak
Director, Program Evaluation and
Information Resources

Enclosures

cc: Keith Galayda
Shirley Malia

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 131 1999

EFFECTIVE DATE: EXPIRATION DATE:

ADMINISTRATIVE POLICY LETTER NO. A97-VI-

FROM: J. DAVITT MCATEER
Assistant Secretary for
Mine Safety and Health

SUBJECT: Internet Policy

Scope
This policy applies to Mine Safety and Health Administration (MSHA) employees.

Purpose
The purpose of this letter is to provide policy guidance for MSHA employees in the appropriate use of the Internet.

Policy
Access to the Internet will be available to MSHA employees, as needed, to carry out work-related duties and responsibilities. The Director of Program Evaluation and Information Resources (PEIR) is the Internet Coordinator for MSHA.

The following constitutes MSHA policy on **use of the Internet** :

1. Employees shall be familiar with MSHA Internet policy and have received Internet training, if necessary, before being granted access to the Internet by their supervisors.

2. Employees shall follow any appropriate software licensing agreements and MSHA software policy when using and/or downloading software resident on the Internet.

3. Employees are to scan any material downloaded from the Internet for viruses.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 132 1999

4. Employees are permitted to download software upgrades or program fixes (patches) available on the Internet only after obtaining permission from the MSHA Software Manager (APL A97-VI-).

5. Employees are to access the Internet as representatives of MSHA for work-related purposes during Government working hours. At no time while accessing the Internet, shall employees exhibit conduct which would damage the reputation of MSHA.

6. Employees who use the Internet in violation of MSHA policy will, as a minimum, lose Internet access.

If an employee does not know what is work-related or has any questions regarding use of the Internet, it is that employee's responsibility to resolve those questions with his or her supervisor before logging on. In addition to losing access to the Internet and possible disciplinary action, there may be legal penalties for abuse of the Internet under provisions of the Computer Fraud and Abuse Act of 1986.

The following policies apply to placing information on the Internet:

1. No information shall be placed on an MSHA Internet site without the following review and authorization:

a. Prior to inclusion on an MSHA Internet site, a document will be reviewed and cleared in the manner established for that type of document; i.e., the established procedure for review, clearance, and signature of any document is not changed because the document will be placed on an Internet site.

Program areas may communicate to their employees specific requirements and appropriate file formats for Internet documents subject to the approval of the Internet coordinator.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 133 1999

b. Any information to be placed on an MSHA Internet site will be authorized by the MSHA Internet Coordinator (Director of PEIR).

2. The Internet is not a secure environment. Therefore, privacy data, as defined by the Privacy Act of 1974, as amended (5 U.S.C. 552a), shall not be placed on an MSHA Internet site.

3. Any MSHA information stored on an MSHA Internet site shall be subject to the same retention and archiving procedures as published public documents (36 CFR 1228.

Background
MSHA is connected to the Internet through its Wide Area Network. It is anticipated that there will be significant information exchange through the use of the Internet.

Authority
APPM Volume VI, Chapter 500 and Volume III, Chapter 200; OMB Circular A-130; the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35; the Computer Security Act of 1987; the Computer Fraud and Abuse Act of 1986 and The Computer Abuse Amendments Act of 1994; the Federal Records Act, as amended; the Privacy Act of 1974, as amended (5 U.S.C. 552a); and the Freedom of Information Act, as amended (5 U.S.C. 552); DLMS IX, Chapter 1200.

Filing Instructions
This policy letter should be filed behind the tab marked "Administrative Policy Letters" at the back of Volume VI of the MSHA APPM.

Issuing Office and Contact Person
Directorate of Program Evaluation and Information Resources
George M. Fesak, (703) 235-8378

Distribution
MSHA Employees
APPM Holders

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 134 1999

EFFECTIVE DATE: EXPIRATION DATE:

ADMINISTRATIVE POLICY LETTER NO. A97-VI-

FROM: J. DAVITT MCATEER
Assistant Secretary for
Mine Safety and Health

SUBJECT: Software Licensing and Management

Scope
This policy applies to all Mine Safety and Health Administration (MSHA) employees.

Purpose
This policy letter establishes MSHA policy regarding software management, documents the legal obligations inherent in the purchase and use of computer software, and advises Agency employees of their responsibility for complying with license agreements.

Policy
The Directorate of Program Evaluation and Information Resources shall have primary responsibility for software management throughout MSHA, including maintaining a software inventory, developing a software audit plan, and administering the implementation of software audits and inventory verification in the Agency. The Chief of the Systems Operations and Communications Division of the Information Resource Center (IRC) shall be the designated software manager for MSHA. IRC shall provide training materials to facilitate implementation of this policy.

The following policy shall be implemented in MSHA subject to the terms of the individual software license agreements:

1. Software acquired by MSHA may not be copied for other than back-up purposes unless permitted in the individual license agreement.

2. MSHA employees shall not use personally-owned software on MSHA computers.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 135 1999

3. No software shall be installed or upgraded on any MSHA equipment or used by MSHA personnel without proof of vendor licensing for the explicit use of MSHA. It is the responsibility of the software installer to determine the existence of a valid license prior to installation. This shall be demonstrated by the presence of an original copy of the software license or the receiving report. In addition, the software must be the proper version listed on the approved MSHA software list (available in the MSHA shared directory on the LAN) or approved by the Information Resource Manager (IRM).

4. All software must be documented on the MSHA software inventory by MSHA employees receiving software. A copy of the receiving report and/or credit card receipt for purchased software must be sent to the MSHA Software Manager in order to maintain a proof-of-purchase audit trail. The following information must be provided to the MSHA Software Manager within 30 days of software receipt and/or installation:

   Name of software and version
   Upgrade or new software
   Software company name
   MSHA office receiving software
   Serial number of computer on which installed (or document as "Not installed")
   Date installed, if applicable
   Date removed, if applicable
   Contact person
   Phone number

   If the software is installed later than 1 week after receipt, an update of the above information shall be provided to the MSHA Software Manager. Provide the same information to the MSHA Software Manager when software is removed from a computer.

5. If a new computer is received with software already loaded, a list of the loaded software, the computer serial number, and a copy of the receiving report must be provided to the MSHA Software Manager within 30 days of receipt of the computer.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 136 1999

6. Users of freeware are responsible for maintaining documentation that the software was acquired and may be used without expenditure of government and/or personal funds. The software should be acquired only from the originator. Since the sources of freeware are volatile, documentation that it is freeware should be acquired at the same time as the software. Provide software inventory information (see item 4, above) to the MSHA Software Manager.

7. Users of shareware (fully functional software that may be acquired and tested without the expenditure of funds for a limited period of time) are obligated to either remove the software at the end of the testing period or acquire a license explicitly for MSHA.

8. Software licensed to MSHA may only be installed in accordance with the license provisions and in the environment for which it was licensed. Software licensed for a stand-alone installation may not be installed on a LAN server unless such installation is specifically authorized by the license and approved by the MSHA Software Manager.

9. Software may not be installed on another computer until it is removed from the current computer. If a computer is purchased with software already loaded, the hardware vendor may require notification or prohibit moving pre-loaded software. The specific license agreement shall be followed regarding notification of the software vendor. The MSHA Software Manager must be notified of any software move (include the information in item 4).

10. Software installed on the LAN, where the license permits a specific number of simultaneous users, shall be metered on the LAN to reflect the limits of the license. This shall be the responsibility of the site LAN manager.

11. Software on the LAN that is only to be accessed by designated workstations, must be protected by granting access permission only to the licensed workstations. This control shall be exercised by the site LAN manager.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 137 1999

12. Software usage shall be periodically audited at each MSHA site in accordance with procedures to be established for the MSHA Accountability Program. When an audit reveals the existence of software without documentation to support a valid license, the software shall be removed from the computer in such a manner that no copy remains. This may be accomplished by erasing the software or un-installing the software and destroying any diskettes used to un-install.

Management and employees share equal responsibility for ensuring compliance with this policy. Non-compliance with this policy could result in disciplinary action by the Agency. Employees are subject to copyright laws and any fines and/or punishment for violating those laws. It is imperative that all MSHA employees understand their individual responsibilities and possible liability regarding these legal obligations.

Background
Computer software is protected by Federal copyright law (Title 17 U.S. Code Section 1 et seq.). The vendor license agreement, provided with the software, details where and how the software may be used.

Authority
Title 17, U.S. Code (Federal Copyright Law);
DLMS 9, Chapter 1200;
Memorandum for All DOL Employees from Patricia Lattimore, Deputy Assistant Secretary for Administration and Management/Chief Information Officer, dated May 19, 1997 - Subject: Reminder on Appropriate Use of DOL Information Technology.

Filing Instructions
This policy letter should be filed behind the Tab marked "Administrative Policy Letters" at the back of Volume VI of the Administrative Policy and Procedures Manual.

Issuing Office and Contact Person
Program Evaluation and Information Resources, Information Resource Center, Sterling K. Townsend, (303) 231-5475, ext. 3220

Distribution
All MSHA Employees
APPM Holders

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 138 1999

Mr. COBLE. Mr. Wrenn and Mr. Smith, I will put this question to you all jointly.

Have computer hackers ever attempted to extort money from either of your companies? In other words, are there instances where someone contacts your company and threatens to help others appropriate a copyrighted work unless there was a payoff?

This is pretty strong language here, but it has ever happened?

Mr. WRENN. Fortunately, to date, it has not happened to Adobe Systems. I do know of two other companies that have faced that. One of them, Symantec, was asked for a million dollars to prevent someone from releasing a utility that would take a trial version of their software that would only work for a certain amount of time and then turn off—this would be what Mr. Smith referred to as a "cracks" type utility—and undo that time bomb and make it a full working copy of the software. They were asked for a million dollars to try and prevent that from being distributed to the Internet.

Mr. COBLE. How about you, Mr. Smith?

Mr. SMITH. It has not happened at Microsoft. I think perhaps one reason is that our policy is very well known in that community, that we would never even think for a moment of negotiating in this context.

Mr. COBLE. Do you know whether or not it has happened in other areas?

Mr. SMITH. I am not aware of any incidents other than the ones that Mr. Wrenn just referred to.

Mr. COBLE. Ms. Sellers, how successful are we at enforcing intellectual property rights overseas?

Ms. SELLERS. The U.S. Trade Representative's office has taken a very strong position, as you probably know, with respect to making sure that other governments live up to the international copyright laws. And we have supported the work of the U.S. trade representative in that effect.

We have also strongly supported the international copyright treaties, particularly the WIPO Copyright Treaty that is pending for implementation.

Mr. COBLE. And I know that we are all—well, strike that. Perhaps not all of us, but many, many of us, from time to time, become very sensitive about maybe inviting retaliation if we, in fact, go hard overseas. To what extent is that a problem?

Ms. SELLERS. The international copyright treaties, at the moment, provide a common denominator for practices across the world. So at this point in time, we are all working towards and in the same direction. And governments ought to be taking the same stand of accountability, and lead by example for their own citizenry.

Mr. COBLE. And Mr. Bono has been involved in this—regarding this next question, and perhaps others on the Subcommittee have, as well.

For what would be your preference at enforcing—the best way to enforce government compliance with our copyright laws?

Would you go with the GAO report, A, or B, Congressional resolution?

Ms. SELLERS. I would begin with a Congressional resolution and an Executive Branch directive.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 139 1999

I do not think at this point in time a GAO study is necessary.

Mr. COBLE. I think at one point, some of you all were advocating a GAO report.

Ms. SELLERS. It could be a possibility, but I do not believe it is necessary at this time.

Mr. COBLE. Very well. I thank you.

The gentleman from Massachusetts.

Mr. FRANK. Ms. Sellers, the issue—you did not quite—I think you answered the question of willful, the concern was that by defining "willfulness" by removing—well, I do not feel removing the commercial equipment—that somehow this might be interpreted as increasing the liability the service provider had, which I do not now have.

My question is, is there any problem with simply making it explicit that we are not trying to do that?

Ms. SELLERS. Well, my problem with adding a blanket exemption, Mr. Frank——

Mr. FRANK. Ms. Sellers, do me the service of answering the question I asked you. Did you hear the word, "blanket exemption," from me?

Ms. SELLERS. No, sir.

Mr. FRANK. The phrase that I gave was simply making clear that this—let me put it to you to you—do you think existing law is a blanket exemption?

Ms. SELLERS. No, sir.

Mr. FRANK. Well, then how is simply stating if this does not change existing law will give people a blanket exemption?

Ms. SELLERS. No. I agree. I think that——

Mr. FRANK. Well, let me ask you——

Ms. SELLERS [continuing]. I am quite happy to say this does not change that law.

Mr. FRANK. My question is would there be any problem with simply making it explicit that this does not change existing law with regard to the online provider liability?

Ms. SELLERS. I do not read the NET Act as changing current law and I do not want to advocate that it changes current law. I believe—I support you in saying that it does not.

My concern with mentioning any of the participants in the Internet community specifically is——

Mr. FRANK. Well, when you say it does not change——

Ms. SELLERS. Right, and I would stop right there. I would not go on to name specific participants in the Internet community because any one of them may engage in pro-active conduct that fits within the willfulness——

Mr. FRANK. Well, then that would be covered by now.

All right. Let me take—I think they are guilty of what they are guilty of——

Ms. SELLERS. Right.

Mr. FRANK [continuing]. Which is overtly your case, which makes me think maybe you got something more online than you do, and I think that there is a mistake.

Yes.

Mr. WRENN. If I may, Mr. Frank, in answer to your question, speaking just for myself, I think it is a good way to approach it,

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 140 1999

because I think what you pointed out earlier is that for a lot of these issues there is unfounded fear. They are not a problem in practice.

I have even had an opportunity in the last week to talk to attorneys from other countries about systematic study. Argentina, Canada, the United Kingdom, they all criminalize even one copy.

But prosecutors are not off hauling out people to jail who really should not go. It is an issue of fear. So if that addresses some people's fear, I think it is a great way to go.

Mr. FRANK. And I think we will have to do that throughout because you cannot take any step forward here without generating some concern that it might go further.

And, look, we have to be clear. Not everybody can control the court, and I think this is a case—there is a great case for being as explicit as possible in doing what we mean to do and not more than that.

Thank you, Mr. Chairman. No further questions.

Mr. COBLE. Thank the gentleman.

The gentleman from Utah is recognized for five minutes.

Mr. CANNON. Thank you, Mr. Chairman.

You spoke so much about "softlifting," but the current Bill that we are dealing with probably does not affect it. The law is pretty much in place for that. The order is to get you a little farther. So we will not try to scare the rest of the world.

Personally, in my private life, I was terrified that we would have people who stole software. Worked very hard to avoid it, and still that happened.

But we are not dealing with that here in this Bill, right?

Ms. SELLERS. No, sir. This is under the oversight hearing concerning software piracy——

Mr. CANNON. Thank you. I have no further questions.

Mr. COBLE. I thank the gentleman.

The gentleman from Massachusetts is recognized for five minutes.

Mr. DELAHUNT. Yes. Thank you, Mr. Chairman.

If we have adequately outlined the fact that there is a very serious problem, then I appreciate—I really do appreciate that testimony.

And maybe I should direct this question to Mr. Kruger or Mr. Wrenn.

In terms of the commercial theft that goes on, and Ms. Sellers, maybe you can answer this, too—has your association or your industry discovered criminal syndicates doing this on a systematic basis in terms of seeking large amounts of ill-gotten gain?

You have?

Mr. WRENN. If I may, I will defer to Mr. Smith, who has more firsthand experience in their investigations at Microsoft with that.

Mr. SMITH. Although it typically at this stage does not relate to Internet piracy, it is absolutely the case today that organized crime is involved in this activity.

Mr. DELAHUNT. I am not talking about the traditional mafia. I am just talking about sophisticated criminal syndicates.

Mr. SMITH. Absolutely.

Mr. DELAHUNT. OK.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 141 1999

Mr. SMITH. But it is of benefit to the Mafia.

Mr. DELAHUNT. Let me ask you this: What do you then do? What is the next step in terms of prosecuting these kind of cases?

Mr. SMITH. When we encounter that kind of case, we typically do some work ourselves initially to put together some amount of information and evidence. But we very early on turned to the responsible agency, whether it is the FBI, the Customs Service, or an overseas agency.

Mr. DELAHUNT. What kind of response do you get?

Mr. SMITH. I think we get a great deal of help and support, especially when there is a broad range of activity or economic impact.

Mr. DELAHUNT. Do you think that they have the sufficient resources available to meet the need? I am talking about agencies under the umbrella of the Department of Justice.

Mr. Kruger.

Mr. KRUGER. There is no question in my mind, Mr. Delahunt, that whatever we do with the *LaMacchia* fix bill, it will never be the case that the U.S. Department of Justice and the Federal Bureau of Investigation will be able to devote sufficient resources to the investigation and the prosecution of software piracy to effectively solve or resolve this problem.

One of the reasons we support this bill is because we think it will have a deterrent impact, not so much——

Mr. DELAHUNT. Right.

Mr. KRUGER [continuing]. We think it will have——

Mr. DELAHUNT. Right.

Mr. KRUGER [continuing]. A practical impact.

But that raises another important point.

In the questioning of the Deputy Assistant Attorney General, you mentioned that there is a concern about making this a Federal offense for making one copy—the theft of one copy a Federal offense.

The Feds are the only game in town. They are the only game. And, in fact, if there is a crime this is it. This is where it belongs.

State and local law enforcement agencies have offered, have approached us about being involved and active on this issue, and unfortunately, because of the Federal preemption as it exists right now, they have no role to play.

Mr. DELAHUNT. Well, you know, maybe it is time that the Department of Justice—of course, I am sure that many of you are unaware of the fact that the Federal Government is now getting more and more into juvenile crime, and I have some very strong reservations as to whether we should be going in that direction. In fact, I do not think we should be going in that direction, and let the states address the problem of violent crime in the communities. At the same time, Federal Government ought to play a role in this particular area because of the fact that it is international in scope. This is where it ought to happen.

Ms. Sellers, I would think that you would want to take your association, sit down with the appropriate officials in the Department of Justice, and ask them to prioritize and to create a task force to deal with this issue.

Ms. SELLERS. You are right, Mr. Delahunt. We have worked very closely with them.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 142 1999

And as a matter of fact, Mr. Di Gregory's Deputy was with us just two days ago, addressing the Committee of the SPA, that oversees our anti-piracy efforts.

We work very hard to prioritize——

Mr. DELAHUNT. We are losing dollars to our national economy here. Let me just—I will conclude with this final question.

What implications does this have for our relationship with other countries with whom we have an extradition treaty?

Does it not provide us a predicate to seek indictments in this country for those in other nations who are pirating our software, our intellectual property?

And Mr. Smith and Mr. Kruger, feel free to address that.

Mr. SMITH. I think it would be very helpful in that context. Other governments are prosecuting people who do this under their criminal laws. The German government, to give you but one example, has been very helpful and vigilant, and it would be helpful if the United States government could play a similar role.

Mr. DELAHUNT. We do not really need a treaty to do this. There are existing extradition treaties out there that we could be using now. I mean we are going to be here debating and discussing, and I am not suggesting that we should not be engaging and participating in international conventions dealing with these issues.

But if you really want to do something, this is an opportunity, I would think, to do it and to do it now.

Mr. SMITH. And I think the sense of urgency is very well put because the reality is that the scope of Internet piracy today is probably twice as broad as it was a year ago, and unless something changes, it will be probably twice as broad a year from now as it is today.

Mr. DELAHUNT. We could add up all the bank robberies that have been committed in the United States of America, and I would suggest that they pale in comparison—in terms of economic loss—to what is happening in this discreet area.

Mr. COBLE. I thank the gentleman.

The gentleman from Indiana is recognized for five minutes.

Mr. PEASE. Thank you, Mr. Chairman.

Most of the questions I was going to ask have already been asked.

Let me just pursue a couple of things that you gave us by way of background.

I am curious as to how you arrive at your figures about the percentage of piracy, both in the United States and worldwide.

I, in a former life, was General Counsel at the university, and we were aggressive in dealing internally with making sure that pirated programs did not show up on our equipment around the university, and it was a constant problem. It took a lot of work and it took a lot of time.

I am wondering how you do that if you do not have internal access to companies or institutions, and how you arrive at these figures.

Mr. WRENN. I think I will speak to the methodology. Both the Business Software Alliance and the Software Publishers Association work with an independent research organization, IPR. In a nutshell, the methodology, which I think is pretty conservative at

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 143 1999

estimating the piracy rate, is based on looking at the number of computers sold in the market and the amount of legal software sold in the market, and then using market research and other data available to determine an average number. These numbers focus mainly on business applications, so we do not really count a lot of the home copying or things like that that go on which is much more difficult to track. If you look at the average number of business applications per computer and at how many computers and applications are actually sold, and you can see the difference as the piracy rate.

There is a whole bunch of computers going out. There just is not that much software going out, and there is pretty good data on that.

So what you come up with then is an indication of what ought to be there for software sales when you compare it to the number of computers available in the market.

Mr. PEASE. Got it.

Do you do any—I understand you will work with companies if they want to do audits within—or somebody will. Maybe the sellers.

Do you do any of this sort of work randomly yourself by your own access to the Internet to see what—where things are being transmitted, where programs are being transmitted?

Is there any auditing of the Internet by either your companies or your associations?

Mr. WRENN. I think actually the associations in both of the companies up here have such a process set up.

We have investigators inhouse at Adobe, for example, and they spend a lot of time tracking piracy, and there is a whole lot of it going on. Unfortunately, we cannot go after every infringing site that we find.

We get a lot of information in our registration data base of companies who are using software who are registering the serial numbers they got off the Internet.

And, I mean, hundreds of thousands—literally hundreds of thousands of registrations that are attempted that should not be there often have addresses in corporate settings.

So, we do monitor this activity and we work with the BSA and the SPA to go after the infringers. Whether it is an end user case and it is being referred for audit or it is one of the few cases, at the moment, that is appropriate for criminal prosecution.

Mr. PEASE. Just an aside. It has nothing to do with this.

Every time you refer to the BSA, my prior life comes forward and I think of the Boy Scouts.

Mr. WRENN. Boy Scouts. Boy Scouts have been a big help to us.

Mr. PEASE. When you talk about the lost—the financial losses——

Mr. WRENN. Yes.

Mr. PEASE [continuing]. Of anywhere from $11 to $20 billion, we heard, is that lost sales that you would have made had those programs not been pirated by someone else, or does that also include your cost of monitoring what is going on and auditing what is happening?

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 144 1999

Mr. WRENN. That is a good question. That data is based on our lost sales——

Mr. PEASE. Only?

Mr. WRENN. Only. Only our lost sales. And, again, it is good because it does not count as a lost sale every copy made by some hacker up at two in the morning on the Internet. Those copies do not count.

We are not saying that every one of those is losing a few hundred dollars for an expensive product. This is for computers installed in businesses. If you have enough money to buy the computer, you have enough money to buy the software. So, it is software in that context where there clearly is an ability to pay for the product, but it has not been paid for.

So that is a good, I think, conservative estimate of dollars lost in the industry in terms of lost sales.

Mr. PEASE. Do either of the associations have any figures that, in addition to the lost sales, the amount of money that you are spending trying to protect copyright—to audit what is going on, to protect your intellectual property rights?

Ms. SELLERS. Well, our enforcement program is on behalf of not only our business application members, which are the ones that are covered by the statistical data, but also our education and entertainment and Internet-based members, as well. And our software piracy efforts really try to address all those situations.

We have not been able to put together any effective statistics as to the dollar losses to those other big industry segments, however, due to the nature of that type of product often being used by individual consumers.

Mr. PEASE. Mr. Smith or Mr. Wrenn?

Mr. SMITH. I would simply add that, just as a company, we are spending just over $40 million per year on education and investigative work related to this problem.

Mr. PEASE. Just your company?

Mr. SMITH. Yes. That is right.

Mr. PEASE. And I realize it is a really big company, but, OK.

Mr. SMITH. It is a lot of money.

Mr. PEASE. Thank you very much.

Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

Thank you all for being with us.

We will invite our final panel to come forward which consists of Cary Sherman, who is the Chief Legal Counsel for the Recording Industry Association of America, a Washington, D.C. based trade association with more than 350 members responsible for creating, manufacturing or distributing 90 percent of all legitimate sound recordings sold in the United States.

Mr. Sherman assists in the development of strategic objectives to achieve the Association's technology anti-piracy, international and government affairs goals.

Many of his responsibilities include reconciling technology and copyright on the Internet, developing industry policy on licensing and enforcement, and coordinating the industry's business and policy objectives for encryption, watermarking and copyright management systems.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 145 1999

Mr. Sherman is also working on mechanical rate negotiations with music publishers.

Prior to joining the RIAA in 1997, he was Senior Partner at the Washington law firm of Arnold and Porter, where he headed the firm's Intellectual Property and Technology Practice Group.

Mr. Sherman obtained his BA from Cornell University and was graduated from the Harvard Law School. Our second witness for this panel is Fritz Attaway, who is Senior Executive Vice President for the Government Relations and Washington General Counsel at the Motion Picture Association of America.

Mr. Attaway joined the MPAA in January of 1976 and was made Vice President of the organization in September of 1978. In 1979, he was named Senior Vice President for Government Relations, and in 1993, became MPAA's Washington General Counsel. He attended the College of Idaho, where he received a BA with honors in 1968.

Mr. Attaway, I am a geographic junkie, but I do not recall the town in which the College of Idaho is located.

Mr. ATTAWAY. 28 miles due west of Boise.

Mr. COBLE. And the name of the town? I knew it was—is there a town there?

Mr. ATTAWAY. Boise is our capital and largest city, and we have—I think Boise has the enormous population of about 150,000 people.

Mr. COBLE. Geographically.

You received your BA degree there with honors in 1968. And in 1970, Mr. Attaway commenced his legal training at the University of Chicago, where he was awarded a National Honor Scholarship. He received his JD degree in June of 1973.

Our final witness is David Nimmer, who is testifying on behalf of the U.S. Telephone Association. Since 1985, he has assumed responsibilities from his father, the late Professor Melville Nimmer of the UCLA School of Law for updating and revising Nimmer owned copyright, the standard reference treatise in the field. Apart from his treatise, Mr. Nimmer authors numerous law review articles on domestic and international copyright issues. He received an AB with distinction from Stanford University, and his JD at the Yale Law School, where he served as editor of the Yale Law Journal.

Mr. Pease, if you would kindly assume the chair. I have to be at another meeting soon, folks, although I will be able to hear some of the testimony. But I will be able to be here for the final hearing.

Pardon? I talked to Mr. Pease earlier. I did not know Mr. Goodlatte was going to be back.

But, gentlemen, good to have you all with us.

Mr. Sherman, if you will kick it off.

STATEMENT OF CARY SHERMAN, SENIOR EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL OF THE RECORDING INDUSTRY ASSOCIATION OF AMERICA

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

The world is listening and the music it wants to hear comes from America. The U.S. sound recording industry is working enthusiastically to broaden our audience around the globe. We want to expose

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 146 1999

the world to jazz and country, reggae and gospel, big band and good old American rock and roll.

Given its immense popularity, American music is also favored by pirates, rampant piracy. It costs the American music industry nearly $1 million a day in the United States and well over $2 billion a year worldwide.

These numbers hit everyone in the music chain. People who contribute their musical talent and genius to make a record, people whose livelihood depend on sound product.

The consumer is the ultimate victim of piracy. When the record companies sustain a financial loss from piracy, there is simply less money to invest in discovering and developing new artists and to subsidize the less profitable types of music, such as classical, jazz and gospel.

With each new technology the industry embraces, vinyl, cassette tape, compact disc, and now the Internet, the threat of piracy only compounds as it has become easier, faster and less expensive to duplicate the creative works of our artists.

In 1991, 12 counterfeiting operations, employing hundreds of individuals, manufactured approximately 28 million counterfeit cassettes.

Today one individual, in less time than it takes me to read this testimony, can send a full-length album to more than 50 million Internet users. The rules of the game have radically changed.

How does all this happen? If you look up on the screen, you will see that personal computers were in 19.1 million U.S. homes in 1985, and of course, by the use of personal computers, give people access to the Internet. By the year 2000, they will be in 154 million homes.

If you look at the purple on the slides, you will see how the Internet has connected virtually the entire planet in the last five years.

Already retailers, record companies, new start-up labels and artists themselves are going online to offer their music directly to the fans.

Here are just a few examples of the new businesses sprouting up all over the Internet. Here is a retailer like Tower, using web sites to enable their customers to place their order electronically and have the CD's shipped right to their home.

Supersonic Boom just announced that surfers can pick their favorite songs and create their personalized CD's.

Another music site lets users check out new bands and artists.

Jaybird Records, the web's first recording label, offers consumers the opportunity to purchase music from the artists signed to the cyber label.

And finally, Music Boulevard has begun to download music directly to consumers selling music electronically instead of on the physical disks.

Unfortunately, the rapid growth of the Internet also means power. Recordings are easily copied to a computer hard drive. Once on the computer, those copies can be uploaded to the Internet with a push of a button, without the knowledge or authorization of the record companies, artists or musicians who created the music. And

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 147 1999

once the recordings are on the Internet, they are available to be downloaded by millions of users.

How do users find these recordings? It is easy. A typical search engine points users to sites, some of which brazenly announce that they offer pirate songs.

This slide shows one of those sites featuring hundreds of full-length songs, listed alphabetically by artists, available for download by anyone, anywhere and at any time.

This is what a download recording sounds like.

[Plays music.]

In case you do not recognize it, this is from the Evita soundtrack, and as you can hear, the sound quality is virtually indistinguishable from that of a compact disc.

Songs by artists such as Mariah Carey, the Rolling Stones, the Police, Sheryl Crow, they are all available for download in near CD quality, and they are all unauthorized.

Here is another example of a pirated site, "John's Take but Don't Tell Page." No doubt about the intent here.

How long would it take you to copy the song we are listening to now?

About the same amount of time it takes to listen to it by using newer cable modem technology that is being mailed out into homes in Alexandria, this song can be downloaded in a fraction of a second. Using a cable modem, a typical CD can be downloaded in just three minutes. And once a user has downloaded those songs, they can be played back at any time, as if the user had actually purchased the music.

Imagine the impact on music creators when their new single is sent up over the Net with the potential of reaching millions of users worldwide with the click of a mouse.

Imagine, also, the impact that pirate sites will have on the legitimate music businesses on the Internet.

Why would anybody buy music from a local retailer or web entrepreneur when the same music is available from a web pirate for free?

What can Congress do to help fight Internet piracy? There are two pieces of legislation currently before the Committee, the No Electronic Theft Act, and the WIPO Copyright Treaties Implementation Act that will help stem the growth of piracy in the United States, around the world and in cyberspace.

The NET Act makes a significant change in the copyright law to provide law enforcement officers with additional tools to prosecute pirates. The requirement in the current law that defendants infringement be for financial gain allows serious incidents of copyright infringement to escape criminal prosecution, the *LaMacchia* case being the quintessential example.

That decision left copyright law defenseless against infringed copyright not for profit, but for the pure fun of it.

Civil lawsuits often do not deter those who wish to steal our music, especially when they view themselves as immune.

The NET Act will help close this loophole for pirates and subject them to possible criminal prosecution. It is a good bill. We support its passage.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 148 1999

We are concerned with a provision that raises the threshold value required to reach a felony conviction because the change would actually operate as an obstacle to criminal prosecution.

By doubling the threshold requirement, the Bill has effectively doubled the work required before an Assistant U.S. Attorney can prosecute the case.

We welcome the opportunity to work with the Committee to ensure that the benefits of the NET Act are realized, and that these commercial-free WIPO Copyright Treaties Implementation——

Mr. COBLE. We will get to that hearing because we are losing a lot of time.

Mr. SHERMAN. What I wanted to say was is the list of importance to stem piracy.

Thank you very much.

Mr. COBLE. Thank you, Mr. SHERMAN.

Mr. Attaway.

STATEMENT OF FRITZ E. ATTAWAY, SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS AND WASHINGTON GENERAL COUNSEL, MOTION PICTURE ASSOCIATION OF AMERICA

Mr. ATTAWAY. Thank you. You all have had a long morning here and I will try not to intrude unnecessarily upon your time.

You have my written statement. The same technology that will smooth the way for legitimate delivery of video on demand over digital networks also will prime the pump for copyright pirates.

Today, the pirate who obtains by stealth or malfeasance a copy of the latest Blockbuster picture even before it is released in theaters must cope with formidable distribution problems. Physical copies must be struggled across borders, warehoused and parceled out to distributors before reaching the ultimate consumer.

Digital networks soon will make this complex and dangerous undertaking cheap and simple. The pirate master will be digitized, posted to the Web, and made available to net surfers all around the world; or, the master will be downloaded over the Internet to an additional video recorder half a world away that can churn out thousands of pristine, perfect copies at the touch of a button for immediate distribution to customers.

As I said earlier, we could go through enormous resources to civilly enforce of our copyrights, but effective anti-piracy action cannot be done without criminal enforcement; and we depend heavily upon law enforcement agencies to enforce copyrights.

You heard earlier from the representative of the Justice Department about Operation Countercopy. I would like to take this opportunity to applaud the Justice Department and the FBI for their efforts against piracy. We look forward to working with them to enforce criminal copyright laws in the Internet area.

The NET Act addresses serious problems created by the *LaMacchia* decision. You have heard what those problems are. I will not repeat them. Suffice it to say that MPAA very strongly supports the NET Act and we urge its rapid enactment.

There is one glitch that I would like to point out—or at least a contingency glitch:

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 149 1999

The courts have interpreted "financial gain" to include the expectation of financial gain, as well as the actual receipt. This interpretation is extremely important to our anti-piracy efforts.

When the duplicating laboratory or warehouse is busted, it may be difficult or even impossible to prove that money actually has changed hands. Of course, there is a clear expectation that money will change hands, even though it has not been received yet by the bad guys.

We urge that the term, "financial gain," in H.R. 2265 be amended to include the term, "Or expectation of receipt." We think that this amendment will fix this potential glitch, which could be very important to us in the future.

In conclusion, I also would like to add our support to the WIPO Implementation legislation. It is very important for electronic piracy control——

Mr. COBLE. We are going to have a hearing about that. You got to be a little respectful about time. We are going to have a separate hearing on that. You will have a chance to talk about it.

Mr. ATTAWAY. I thank you for your time.

[The Statement of Mr. Attaway follows:]

PREPARED STATEMENT OF FRITZ E. ATTAWAY, SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS AND WASHINGTON GENERAL COUNSEL, MOTION PICTURE ASSOCIATION OF AMERICA

Chairman Coble, Representative Frank, and members of the Subcommittee: My name is Fritz Attaway, and I am Senior Vice President and Washington General Counsel of the Motion Picture Association of America (MPAA). I appreciate this opportunity to present MPAA's views on copyright piracy on the Internet, and on H.R. 2265, the No Electronic Theft (NET) Act.

Over the years, MPAA and its members have, to our chagrin, become intimately familiar with trends and developments in the field of copyright piracy. Today, piracy of audio-visual products—movies, videos, television programs—is a $2 billion a year problem worldwide, and growing. We are fighting it with hundreds of investigators, technicians, and lawyers, at a cost of millions of dollars, in almost 80 countries around the world. Copyright piracy *on the Internet* is not a big problem for the motion picture industry—yet. But we know that it soon will be a gigantic problem, inflicting losses that threaten to dwarf the dollar amounts we lose today.

For that reason, we applaud you, Mr. Chairman, for holding this hearing, and we commend Representative Goodlatte and his cosponsors for their leadership in introducing the NET Act. Its rapid enactment will improve the legal weapons in the arsenal of federal prosecutors and law enforcement personnel as they seek to enforce the criminal provisions of the copyright law against a new breed of cyberspace pirate.

Before I explain why we support this legislative initiative, let me take a moment to specify what we are talking about when we refer to "copyright piracy."

The copyright law gives the producers of motion pictures a set of exclusive legal rights. These include the right of public performance—for example, the right to show a movie in a theater, or to broadcast a program on television. They include the right of distribution—the right to sell or to import pre-recorded videocassettes or laser discs, for instance. And these rights include the fundamental exclusive right to reproduce copies of audio-visual works: for example, to copy a motion picture onto videocassette, or laser disc, or the latest new medium, Digital Video, or Versatile, Disk (DVD)—so that those copies can be sold, rented, or distributed in other ways. Of course, all these exclusive rights apply on the Internet as well. Only the producer of an audio-visual work can authorize it—or any substantial part of it—to be copied onto a World Wide Web site, or transmitted across the network, or performed or downloaded by a computer or other device half a world away.

Exploiting these exclusive rights—either exercising them ourselves, or licensing someone else to exercise them—is the main way that a motion picture studio earns its revenue. That's how we pay for the skyrocketing costs of motion picture production and distribution—a cost that more and more often shoots beyond the $100 million dollar mark for a single picture, and sometimes twice that high. Copyright

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 150 1999

underlies the paychecks for the hundreds of thousands of jobs our industry generates, directly or indirectly—everyone from the superstars to the store clerks in the video shop on the corner.

It's no exaggeration to say that without copyright, there would be no movie business. So whenever other people, without our permission and without compensation to us, go into the business of exercising these exclusive rights, they are stealing our intellectual property and robbing the writers, actors, costume designers, electricians, carpenters, truck drivers, theater ticket takers, TV station engineers and hundreds of thousands of others whose livelihoods are dependent on our industry.

With that capsule summary of "copyright," we come to the subject of "piracy." That's what we call it when someone else makes it their business to exercise our exclusive rights, often on a massive scale, and almost always for financial gain.

We're not talking here about the isolated instance of copyright infringement, the company or institution or individual that sometimes steps over the line onto our property rights. We're certainly not talking about the kinds of activities that could, under the right circumstances, qualify as fair use, and that therefore may fall outside the scope of copyright enforcement altogether. Piracy is organized, deliberate and intentional theft of our intellectual property. It is a business—and, as I have mentioned, a very big business around the world. In many countries, the pirate is our toughest competitor—if you can imagine a competitor who pays virtually nothing for his most valuable raw material, who never pays taxes or observes regulations, who often mixes his work with other kinds of organized criminal activity, and who never plays fair. No wonder piracy is the most significant market access barrier we must overcome in bringing U.S. audio-visual products to many markets around the world.

Copyright piracy of audio-visual products takes many forms, and MPAA is experienced at fighting all of them: purloined prints for theatrical performances and master copies; unauthorized broadcast or cable transmission of programs; production and sale of pirate videocassettes and laserdiscs. Last year alone our worldwide anti-piracy operations conducted almost 25,000 investigations, initiated almost 6000 legal actions, and seized over four and half million pirate videos.

New technology continues to confront us with new anti-piracy challenges. Today, those new challenges focus on digital media. In Asia, that often means the video compact disk (or VCD), two CD-sized disks that can carry a full-length movie. Increasingly, piracy of digital media will affect the exciting new format, DVD. But we know that, tomorrow, we must be prepared to grapple with a new form of piracy—and with a new breed of pirate.

Internet piracy is not a "maybe" problem, a "could be" problem, a "might someday be" problem. It is a problem—a serious one—here and now. In odd corners of the World Wide Web, in linked sites based in Europe, Asia and Australia as well as the U.S., a virtual pirate bazaar is underway. Its customers span the globe, wherever the Internet reaches, and its wares are the fruits of American creativity and ingenuity.

Today's fledgling marketplace for Internet piracy has some peculiar characteristics. For one thing, in many transactions, no money changes hands in return for the delivery of illicit copies. Some outlaw bulletin boards operate on a barter system, in which participants swap the latest hot items. In other cases, financial arrangements are masked as subscriptions or access fees. And some people seem to commit Internet piracy, not for money, but for fun: for the challenge of picking electronic locks, for the thrill of intruding into private or proprietary areas, for the buzz of getting away with it.

Today, Internet piracy focuses on computer programs, videogames, and, increasingly, recorded music. Movies and videos are not much in evidence—yet. That's because our audio-visual content is so rich in information that it can't yet move easily everywhere in the digital network—the volume of flow is too great for some of the pipes. We know that the reprieve is temporary, however. The same technology that will smooth the way for legitimate delivery of video on demand over digital networks will also prime the pump for copyright pirates. And they won't be just the thrill seekers and amateurs we tend to hear about today.

We can be certain that the Internet will be the crucial link in the pirate operations of tomorrow. Today, the pirate who obtains, by stealth or malfeasance, a copy of the latest blockbuster picture before it is even released in the theaters must cope with formidable distribution problems. Physical copies must be smuggled across borders, warehoused, and parceled out to distributors before reaching the ultimate consumer. Digital networks will soon make this complex and dangerous undertaking cheap and simple. The pirate master will be digitized, posted on the Web, and made available to Net surfers all over the world. Or, the master will be downloaded over the Internet to a digital video recorder half a world away, that can churn out thou-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 151 1999

sands of pristine, perfect copies at the touch of a button, for immediate distribution to customers. By the time those pirate DVD copies hit the street, the pirate web site will have disappeared, to be set up anew tomorrow in a different country, where a different current hit will be available.

The challenge facing MPAA—and, indeed, all the copyright industries—is to ramp up our efforts against Internet-based piracy before this chilling scenario becomes a reality. We must attack this problem on a number of fronts. Industry will continue to commit its resources and its energy to the anti-piracy effort, of course. But we will also need the help of this subcommittee, and of the Congress, if these efforts are to succeed. Let me explain why.

For many years, MPAA has enjoyed an exceptional working relationship with the Federal Bureau of Investigation and other federal law enforcement agencies in the fight against copyright piracy. I am pleased to report to you that the Department of Justice recently upgraded its efforts in criminal enforcement of the copyright law. It has established a Computer Crime and Intellectual Property Section within the Criminal Division, and stepped up its training activities for federal prosecutors in the area of copyright piracy. Last May, in coordination with the FBI, the Justice Department announced "Operation Counter Copy," in which 35 indictments were returned against copyright and trademark pirates across the country, including several involving video piracy.

MPAA applauds the work of the Justice Department and the FBI in this area, and we look forward to working with them to enforce the criminal copyright laws in the Internet arena. But we know that their anti-piracy efforts—as well as our own—are hampered by flaws in the legal framework for combating Internet-based copyright piracy. Those flaws are epitomized by the 1994 U.S. District Court decision in *United States* v. *LaMacchia*. The defendant in that case operated a bulletin board through which one million dollars worth of pirated software was distributed. The court dismissed a wire fraud prosecution against Mr. LaMacchia because it had not been alleged that he personally profited from this scheme.

How will this decision affect the interpretation by courts of the statutory requirement to prove "commercial advantage or private financial gain" in order to establish a criminal violation of the Copyright Act? That has been a topic of lively discussion among prosecutors and lawyers ever since the decision was handed down, but to some degree the debate is beside the point. Whatever its formal impact as precedent, the well-publicized *LaMacchia* decision has been widely viewed among one category of Internet denizens as providing a "hacker defense" to prosecution for piracy. Until this decision is firmly disapproved, the perception will be all too widespread on the Net that, so long as no money changes hands, it's open season on the intellectual property of others.

That's where the NET Act comes in. It closes the *LaMacchia* loophole, in two ways. First, it makes clear that "financial gain," for the purpose of the criminal copyright law, includes receiving anything of value. Second, it allows pirates to be prosecuted, not just on the basis of how much money they have pocketed, but on the basis of how much they have stolen from copyright owners.

There is one glitch in H.R. 2265 that I would hope you can fix before this bill becomes law. The courts have interpreted "financial gain" to include the *expectation* of financial gain. This interpretation is extremely important to our antipiracy efforts. When a duplicating laboratory or warehouse is busted, it may be difficult or even impossible to prove that money has actually changed hands. Of course, there is a clear *expectation* that money will change hands, even though it has not yet been *received* by the bad guys.

Thus, it is very important to us that the definition of financial gain in H.R. 2265 be amended to read "The term 'financial gain' includes receipt, *or expectation of receipt,* of anything of value, including the receipt of other copyrighted works."

These changes are an appropriate and measured response to new means of copyright piracy, and to new breeds of copyright pirate. Copyright generates the revenue stream that makes possible the enormous investment required to bring quality audio-visual entertainment to screens around the world—cinema screens, television screens, and, increasingly, computer screens. If a pirate diverts that stream by unlawfully exercising the copyright owner's exclusive rights, his exposure to prosecution shouldn't depend solely upon whether he, personally, drinks from the stream. The motion picture industry and its employees—and, ultimately, the viewers who await the next great movie—are harmed by piracy, whether or not the pirate profits.

The NET Act also contains other modest amendments that will help courts to sentence copyright pirates more realistically, on the basis of better information about the real impact of the crimes for which the defendants have been convicted. Altogether, enactment of this bill will significantly enhance the ability of the Justice De-

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 152 1999

partment, FBI and other law enforcement agencies to crack down on copyright piracy wherever it occurs—on or off the Internet.

The NET Act is no panacea, of course. Other changes to U.S. law are needed to bring our anti-piracy arsenal up to date. Another bill pending before this subcommittee would accomplish this. H.R. 2281, the WIPO Copyright Treaties Implementation Act, will make the changes in U.S. law that are needed for our country to join the two new copyright treaties negotiated last December. It includes essential provisions outlawing the trafficking in circumvention devices and services—high-tech burglar's tools—that are used to break through technical measures that copyright owners use to control access to, or copying of, their works. Getting this protection on the books will be a dramatic setback for Internet-based pirates, and for those who are already gearing up to make illegal copies of audio-visual works in the exciting new DVD format. The U.S. should lead other nations into compliance with the new WIPO treaties, and thus send the message around the world that copyright is alive and well in the evolving global electronic marketplace. Prompt action on H.R. 2281, without extraneous amendments, will demonstrate that leadership.

Thank you for giving me the opportunity to share these views with the Subcommittee today.

Mr. COBLE. Thank you, Mr. Attaway.

Mr. Sherman, before I leave, I know Mr. Frank is in a hurry to get out of here, but Mr. Attaway, you said about intruding on our time. I do not want any of you to feel that you are intruding on our time. That is why we are here.

But we do try and deal with the five minute roll. I appreciate that, particularly as to your oral testimony. Music is——

Mr. PEASE. [presiding] Mr. Nimmer.

STATEMENT OF DAVID NIMMER, IRELL AND MANELLA, LLP

Mr. NIMMER. Thank you, Mr. Chairman, and thank you to all members of the Committee for the honor of testifying here today on behalf of the United States Telephone Association.

The USTA supports the spirit of the NET Act, as I believe all the witnesses who have testified today have. In addition, the USTA joins with some of the witnesses who have testified in the first session in noting that some of the provisions of the NET Act are overly broad.

The USTA supports the spirit of this Bill, inasmuch as the telephone companies that comprise the United States Telephone Association own a tremendous amount of intellectual property, along with organizations of the other speakers on this panel, and yet those telephone companies also function as the Internet service providers, providing the hardware and the software and the instrumentalities that allow the Internet to run. And from that dual perspective, we would like to share our thoughts with you this afternoon.

We support the Bill, provided that language along the lines of the fix contained in my written proposal is adopted; and I refer to the language on page 4 of my proposal, and I thank the Committee for accepting that full written statement.

This language is narrowly crafted. It is aimed in particular at the *LaMacchia* prosecution that failed, and it aims to remedy the loophole in existing law.

It is not broadly drafted to sweep new parties within its scope, and I would also add that in light of the colloquy that went on this morning about the word, "willfulness," one facet in particular of our proposal is that it avoids the need to define that term altogether.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 153 1999

Thus, USTA would join with those witnesses who do not support a special definition for "willfully," provided that that term is not used in the context of this Bill.

I would like to enter the fray, if I might, in which Register Peters found herself this morning with several members of this Committee to address the question, "What is the problem with this Bill?" In order to address that situation, we need to compare it with current law.

Currently, one is culpable of criminal copyright infringement so long as, one is culpable of civil copyright infringement and two, additional elements are present: First, commercial benefit, and second, willfulness.

Now, I listened with great interest several moments ago when Congressman Frank dismissed the defense that an OSP would have under current law based on commercial benefit.

As we heard from Congressman Frank, because OSP's charge a set amount of money, they would be within the scope of the first requirement commercial benefit under current law. Let us examine that supposition for a moment.

It is true that OSP's and ISP's charge perhaps $20 a month for unlimited access to their services, and it is true, sadly, that a small amount of the material that flows over the Internet consists of copyright infringement.

The logic we heard is that because of that $20 a month coming in, the OSP's would find themselves culpable under the first standard without being able to interpose the defense "we did not make a surcharge of $100 for any copyright infringing material."

Moving to the second standard, willfulness, our fear is that precisely that the same logic will prevail in that context. In other words, the OSP, facing a criminal copyright indictment, would say, "We did not willfully infringe the copyright laws. We had no intent to put infringing material, per se, on our services." And we feel that the very same logic would be thrown back in our face, namely. "You did operate an OSP. You did not do that accidentally or negligibly. We did not find your services purloined by a rogue individual to run an ISP on the site. You deliberately ran an ISP. You intentionally ran an ISP, and you knew that some of the materials that would go over that ISP would constitute copyright infringement."

It is that precise logic that leads us to fear the consequences of this Bill, and on that basis, to offer a solution.

Now let us look at the two proffered solutions, apart from the one offered by USTA that had been discussed earlier today.

The first solution was when Register Peters mentioned—and she only had a moment to do so, in fairness to her—the passive carrier exemption. It is very useful to focus on that because that does not have anything to do with criminal copyright liability, per se.

Instead, the passive carrier exemption states that when, let us say, a cable company simply puts unaltered the signal from a television station over its facilities, it is not culpable for any copyright infringement, civil or criminal.

We could support a fix parellel to that passive carrier exemption, however, we would note that such an exemption for OSP's is not

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 154 1999

the status under current law. for this purpose, I refer the subcommittee to *Playboy* v. *Frena,* covered in my written statement.

The second fix, and I will be very quick now since I see my time is almost over, Mr. Di Gregory stated on behalf of the U.S. Department of Justice that the DOJ is not intending to go after the ISP's of the world.

Well, I know when I was a Federal prosecutor in charge of copyright prosecutions, it was very difficult to interest the FBI in these matters. We have seen a sea of change today when Mr. Di Gregory testifies that this is a top priority of the Department of Justice.

Our concern is combining a top priority of the Department of Justice with amorphous language coming from the Congress of the United States leads to the potential for great mischief to the ISP's and OSP's of the world, and hence, to the Internet that we all wish to foster today.

Thank you very much.

[The Statement of Mr. Nimmer follows:]

PREPARED STATEMENT OF DAVID NIMMER, IRELL & MANELLA, LLP

Good morning, Mister Chairman and Honorable Members of the Committee. My name is David Nimmer, and I am honored to have been invited here today, to testify on behalf of the United States Telephone Association.

The proposal in H.R. 2265 to amend the criminal provisions of the Copyright Act arises at an historic moment. For 1997 marks the centenary of the first criminal penalties for copyright infringement. Specifically, in 1897, Congress provided that the criminal reach of the Copyright Act extends to infringement that is both "willful" and undertaken for profit. Act of January 6, 1897, ch. 4, 29 Stat. 481–482. Every subsequent enactment in the criminal copyright sphere to date has retained both of those statutory elements as a predicate to holding infringement criminally actionable. *See* 17 U.S.C. §506(a); *United States* v. *Moran,* 757 F. Supp. 1046, 1049 n.2 (D. Neb. 1991) (statutory meaning has remained the same over time, even as the language has changed).

Technology, meanwhile, has advanced dramatically. The last hundred years have witnessed the growth of the recording industry, the motion picture industry (and its offspring, the home video industry), and the computer software industry. Each of these technologies gave rise to unique copyright concerns, and, to each of these concerns, Congress provided a legislative response.[1] Today we confront the phenomenon of the Internet—not so much a new technology as a technological revolution itself—and the concomitant copyright concerns unique to the online environment.

One such concern that has attracted substantial attention recently is that some harmful copyright infringement taking place over the Internet, which logically should be subject to criminal penalty, in fact is not under current law. For example, under current law, a computer user who intends to subvert copyright protection—but who acts in the spirit of "malicious mischief" rather than for personal pecuniary advancement—escapes criminal liability. That scenario unfolded in *United States* v. *LaMacchia,* 871 F. Supp. 535 (D. Mass. 1994), in which a young M.I.T. student loaded a large volume of copyrighted material onto the Internet, making it available *gratis* to anyone with a modem. Because the defendant derived no personal benefit from his conduct, the traditional criminal statute did not reach his particular variety of copyright infringement.

H.R. 2265 (the "No Electronic Theft" or "NET Act") attempts to patch the hole exposed by the *LaMacchia* case. The United States Telephone Association approves the spirit animating this legislative fix; USTA-member phone companies hold substantial intellectual property, ranging from directories to software to traditional literary and audiovisual works. As such, they strongly wish to preserve the value of

[1] Congress granted sound recordings full copyright protection in 1971. In 1982, Congress increased the penalties for criminal infringement, in response to lobbying by the Motion Picture Association and the Recording Industry Association. In 1992, Congress extended the felony provisions of 18 U.S.C. §2319 to the criminal infringement of copyrighted computer software. A constant throughout these various legislative changes is that none altered the twin requirements of "willfulness" and profit motivation as the two prerequisites to the existence of criminal copyright infringement.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 155 1999

their billion-dollar portfolios through appropriate copyright protection, including criminal sanctions. To the extent that a loophole in the law as currently formulated allows parties to engage in widescale infringement via the Internet today so long as they lack the type of profit motivation that historically underlay all such widescale infringements in the past, the statute is now ripe for amendment.

At the same time, however, USTA is concerned that H.R. 2265 goes much further than its stated goal. In the process of widening the criminal net to capture those who have evaded its reach only because of an historical anomaly, the bill spreads its reach too widely, jeopardizing in the process actors whose conduct in no sense warrants invocation of the criminal sanction.

Language of H.R. 2265 and Suggested Alternative Proposal

Turning to the particulars of H.R. 2265, the bill defines as criminal the activity of "[a]ny person who infringes a copyright willfully . . . by the reproduction or distribution, including by electronic means, of 1 or more copies, of 1 or more copyrighted works."[2] Two salient particulars of that formulation deserve attention. First, it retains the word "willfully" for criminal copyright infringement—but it does not define what that key term means in the new context of the Internet. Second, it allows for criminal culpability even in the absence of "commercial advantage or private financial gain."

Before analyzing each of those features in some depth, it is useful to hold in mind as a counterpoint the following alternative language that could be included in any bill to redress the problems engendered by the *LaMacchia* opinion:

> Whoever places copyrighted, commercially-marketed material on a computer system with the intent that it be accessible by the public without the consent of the owner of the copyright shall be punished as provided [by law.]

Willfulness

One defect of H.R. 2265 is that it leaves ambiguous the potential criminal liability of Internet Service Providers whose users place copyrighted material online. By contrast, the alternative proposal set forth above clearly delineates the lack of criminal exposure of those same ISPs. The trouble with the proposed legislation begins with the word "willfully." As in previous instantiations of Section 506(a), the term "willfully" is not defined in the text of the statute. Nor is it self-defining in the Internet context to which the aptly-named NET Act pertains.

Whereas in years past the contours of copyright infringement in traditional media may have been relatively straightforward, such that no definition of "willful" was required, at present the notion of what activity constitutes copyright infringement in the context of the Internet is the subject of hot debate. The scholarly literature shows a wide range of opinion as to what activities may render ISPs in particular liable for infringement, on theories of both direct and indirect liability. In addition, the case law on the subject is divided. For precisely these reasons, H.R. 2265—representing one of Congress' first efforts at regulating copyright infringement in the Internet context—must define its key terms as they apply to the radically new realm of cyberspace.

Definition of Willfulness

"Willful," as the Supreme Court has recognized, is "a word of many meanings," *Ratzlaf* v. *United States*, 510 U.S. 135, 141 (1994).[3] The legislative history of Section 506(a) fails to clarify which of those "many meanings" Congress intended the statute to carry. *See Moran*, 757 F. Supp. at 1049 n.2.

Lacking guidance from Congress, the courts have interpreted the willfulness element of Section 506(a) differently. *See Moran*, 757 F. Supp. at 1049 (collecting

---

[2] One matter beyond the scope of this presentation at least deserves mention. The wording of proposed 17 U.S.C. §506(a)(2) suggests that transmission of digital information over the Internet implicates the copyright holder's distribution right, in addition to the reproduction right. The NET Act thereby resolves a controversial issue that has previously excited heated debate. The Working Group on Intellectual Property Rights endorsed that particular construction in its 1995 White Paper, *see id.* at 213; but legislation introduced to implement the White Paper's proposals died in committee during the 104th Congress. The USTA respectfully submits that this particular debate over which of copyright's several rights finds itself implicated over the Internet deserves to be resolved cautiously and deliberately, after a full hearing on the consequences of adopting any particular viewpoint. A tacit assumption embodied in the drafting language of the NET Act is an inappropriate vehicle to resolve this substantive controversy.

[3] No less an authority than Learned Hand decried its use in criminal statutes: "It's an awful word! It is one of the most troublesome words in a statute that I know. If I were to have the index purged, 'willful' would lead all the rest in spite of its being at the end of the alphabet." Model Penal Code and Commentaries, §2.02, at 249 n. 47 (Official Draft and Revised Comments 1985) (quoting ALI Proceeding 160 (1955)).

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 156 1999

cases). The minority view holds that "willful" means only an intent to copy, not an intent to infringe. *See United States* v. *Taxe,* 380 F. Supp. 1010, 1017 (C.D. Cal. 1974), *aff'd,* 540 F.2d 961 (9th Cir. 1976), *cert. denied,* 429 U.S. 1040 (1977). The majority view is that "willfully" means a "voluntary, intentional violation of a known legal duty." *Moran,* 757 F. Supp. at 1049.

The courts' divergent interpretations of Section 506(a) yield uncertainty; they result in similarly-situated persons being treated differently. Legislation targeting the Internet—which has a nationwide user-base, and which knows no jurisdictional boundaries—requires a uniform interpretation. This is particularly true when criminal prosecutions are at stake: the government must provide clear notice of what conduct is subject to criminal punishment.[4] Accordingly, as an initial step in clarifying the intended reach of H.R. 2265, Congress should specify that "willful" in Section 506(a) requires specific intent to violate a known legal duty. That clarification would bring the statute into line with general principles of criminal law. *See Brock* v. *Morello Bros. Construction, Inc.,* 809 F.2d 161, 164 (1st Cir. 1987) ("In the criminal law, 'willful' conduct typically means that the offender not only intended to perform the unlawful act, but also that he know that what he did was unlawful") (Breyer, J.).

Application of Willfulness

It is not enough, however, merely to specify that Section 506(a) requires specific intent to violate a known legal duty. When the contours of a legal obligation are themselves in doubt, the definition of "willfulness" gyrates accordingly. *United States* v. *Garber,* 607 F.2d 92, 98 (5th Cir. 1979) (*en banc*). At present, Congress has not defined the duty of an ISP when one of its users commits copyright infringement online. So long as that duty remains undefined, the proposed changes to Section 506(a) leave unresolved the issue of ISP criminal liability for its users' online infringement.

A case in point is *Playboy Enterprises, Inc.* v. *Frena,* 839 F. Supp. 1552, 1554 (M.D. Fla. 1993). The court in that case found the defendant operator of a computer Bulletin Board Service liable for direct copyright infringement when a BBS subscriber uploaded copyrighted material to it. Thereafter, in *Sega Enterprises Ltd.* v. *MAPHIA,* 857 F. Supp. 679, 683 (N.D. Cal. 1994), the court enjoined the defendant BBS operator whose users uploaded copyrighted material, this time on a theory of contributory infringement. By contrast, in *Religious Tech. Ctr.* v. *Netcom On-Line Comm. Servs., Inc.,* 907 F.Supp. 1361 (N.D. Cal. 1995), the court drew the line for liability more narrowly, holding an ISP immune from direct infringement, and leaving open the question of liability on a theory of contributory infringement. *Id.* at 1381.

The lesson from that trio of cases is that standards are only beginning to emerge for the level of duty that an ISP bears with respect to copyright infringement that crosses its services. Moreover, the different standards articulated by the district courts have yet to reach appellate review.

In such a climate of confusion, the danger facing an ISP is that it can have no certainty, for example, that the standard enunciated in *Playboy Enterprises, Inc.* v. *Frena* will be rejected by other courts. *See Nimmer on Copyright* § 12.04[A][3][e] (exposing doctrinal inadequacies of *Playboy* standard). The possibility therefore remains that a United States Attorney will determine that ISPs who do not comport themselves with the obligations assumed by the Playboy court are acting in derogation of a known legal duty. Under that scenario, the only thing standing between the company and an indictment is the exercise of prosecutorial discretion, a capricious fate on which no company can stake its fortunes.

As an alternative scenario, it sometimes happens that a party informs an ISP that it believes its copyright is being infringed in a certain location of cyberspace, as occurred in *Religious Tech. Ctr.* v. *Netcom.* 907 F. Supp. at 1366. If the ISP responds by disabling access to that site and it later turns out that the notification of infringement was erroneous, then the ISP risks liability to the party whose material was wrongly disabled; conversely, if the ISP declines to undertake that disabling, then it risks being called to account for the intentional violation of a known legal duty. That last scenario in turn raises, once again, the specter of indictment under the NET Act.

At first blush, those last considerations may appear to touch solely on the sphere of civil liability for copyright infringement. But that appearance is mistaken. For in

[4] In Professor Fuller's famous formulation, "The desideratum of clarity represents one of the most essential ingredients of legality." Lon Fuller, *The Morality of Law,* 63 (1969). This rule is reflected in the Constitution's requirement of due process and its prohibition on *ex post facto* laws.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 157 1999

defining the contours of the NET Act, reference to civil liability is inevitable. The cases are legion in which courts exposit the proper reach of a criminal copyright indictment by reference to the standards of civil copyright infringement. *See, e.g., United States* v. *Manzer*, 69 F.3d 222, 227 (8th Cir. 1995) ("In order to understand the meaning of criminal copyright infringement it is necessary to resort to the civil law of copyright."); *United States* v. *Cross*, 816 F.2d 297, 303 (7th Cir. 1987) (same).

By the same token, an equal and opposite reaction pertains. To the extent that Congress specifies the standards for criminal liability in the Internet context, spillover to civil cases arising in the same sphere is inevitable.

Because of the inherent interrelationship between criminal and civil standards for copyright liability, it follows that the issue of ISP criminal liability cannot be resolved by piecemeal legislation. What is required is a considered appraisal of the larger policies at stake. The danger that the NET Act, as currently drafted, poses to ISPs and others—whose facilities may be used to commit copyright infringement on the Internet—must be defused to foster growth of the Internet itself.

Discarding of "For Profit" Requirement

The second noteworthy feature of the NET Act is that it allows for criminal copyright infringement even in the absence of commercial advantage or private financial gain. USTA agrees that the *LaMacchia* example points to the need for some amendment in this regard.

The concern with the approach of the NET Act is its breadth. Putting aside the question whether two neighbors who swap over the back fence computer diskettes that each purchased at Egghead Software are really appropriate candidates for Leavenworth, one need not go as far as the NET Act to indict the LaMacchias of the world. Instead, the Alternative Proposal set forth above accomplishes the same goal less obtrusively.

In calibrating the reach of the NET Act, it is worth considering again the facts set forth in round two of *Religious Tech. Ctr.* v. *Netcom*. In that case, Dennis Erlich, a disgruntled ex-Scientologist, posted to the Usenet some of the secret writings by L. Ron Hubbard. The district court concluded that his wholesale copying of those materials, for the purpose of ridiculing with little added commentary, exceeded the bounds of fair use. 923 F.Supp. 1231, 1249–50 (N.D.Cal. 1995). A case raising similar facts, but which reached the opposite conclusion on the fair use defense is *Belmore* v. *City Pages, Inc.*, 880 F. Supp. 673, 678–79 (D. Minn. 1995) (wholesale copying of plaintiff's copyrighted work, for the purpose of ridiculing with little added commentary, defensible as fair use).

The juxtaposition of *Netcom* with *Belmore* reveals that reasonable minds can differ over the scope of civil copyright infringement under similar facts. What united both those cases is that the copyists acted to make a political point, rather than from commercial motivation. Thus, both would be immunized from criminal liability under current law.

But with passage of the NET Act, not only is Dennis Erlich civilly liable to the publishing arm of the Church of Scientology, but his conduct becomes criminally actionable as well. That startling result goes well beyond the need for a fix pointed up by the *LaMacchia* case. By contrast, if gauged by the alternative language proposed above, then David LaMacchia's posting of commercial software would become criminally liable, whereas Dennis Erlich's postings of L. Ron Hubbard's writings would remain actionable solely in the civil sphere. It is submitted that that last result comports with sound policy and common sense.

Conclusion

Given the design of the Internet, ISPs make numerous automatic and often temporary copies of the materials that their users disseminate online. If ISPs were liable to criminal prosecution for every act of infringement that traverses their networks, merely because they provide the wires and software as "on- and off-ramps" to the information superhighway, the danger arises that the Internet itself could be prosecuted out of existence.

Presumably, that draconian, indeed absurd, result is not the conscious intent of the bill. If that assumption is correct, then USTA submits that the ambiguities in H.R. 2265 should be removed, and Congress' intent should be clarified that the criminal sanction is not intended to apply to ISPs acting in the ordinary course of their operation. The need for careful framing of the issues in this legislation is especially keen in light of specific proposals, currently before this subcommittee on a separate bill, to create safe harbors for ISPs whose users may commit copyright infringement over their networks.

Regardless of which approach is ultimately adopted on the civil side, it is essential to conceptualize both civil and criminal liability simultaneously when crafting new

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 158 1999

"rules of the road" for the Infobahn. For better or worse, the NET Act will be consulted by courts when calibrating liability—both civil and criminal—for copyright infringement that takes place on the Internet. For that reason, USTA respectfully urges that it is inadvisable for Congress to legislate liability on a blank page, as does the current bill. Instead, H.R. 2265 should be redrafted along the lines of the Alternative Proposal set forth above to plug the hole created by the *LaMacchia* case, and due deliberation should be paid in later legislation to the larger issue of liability in the Internet context.

Mr. PEASE. Thank you very much, also, Mr. Nimmer.

I want to follow up. In your written testimony, you propose a fix, as you categorize it, for the legislation, and you refer there to registration of the material. Can you explain more fully for me what you mean by that, and whether—can you explain more fully for me what you mean by that?

Mr. NIMMER. Yes, Mr. Chairman. The current language on page 4 has deleted from it the requirement of registration, but you are quite correct in that the initial version did have a requirement of copyright registration. I apologize for any confusion engendered by the change.

Mr. PEASE. OK. Thank you.

Mr. Frank for five minutes.

Mr. FRANK. Thank you.

Mr. Nimmer, I am a little puzzled. Are you differing with my view about commercial?

Is it your view that the definition of "commercial" means only if you can be shown to be charging an additional sum for an additional item?

Mr. NIMMER. Well, of course, Congressman, that goes to the commercial benefit.

Mr. FRANK. Yeah.

Mr. NIMMER. But, Congressman, the problem——

Mr. FRANK. This commercial—your point—I am just puzzled by—are you maintaining that that is not the case with regard to these providers?

Mr. NIMMER. If an OSP were to be indicted under——

Mr. FRANK. No. I am not talking about whether they are indicted. I was talking about just your description that you seem to be implying that you should not be found to be in something for commercial gain unless you can show that there was an increment additionally charged for each item. If there is an ongoing business, you could not be accused of charging for commercial gain for any particular item.

Mr. NIMMER. That will be a defense under current law that the—such infringement that took place was not destined for commercial gain. It simply happened incidentally without any commercial gain.

Mr. FRANK. For *LaMacchia,* that is what we are trying to change.

Mr. NIMMER. That is correct.

Mr. FRANK. Yeah. The feeling that certain ability to fix two problems that I see. One, why only commercially-marketed material? Why should not the copyright owner have a right to reserve the option to herself?

Mine are to commercially marketed. If I had not commercially marketed and I planned to, you would let them off.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 159 1999

Mr. NIMMER. The problem is that copyright law is so broad today, it includes even a drawing made by my kindergartner as soon as she takes the crayon off of the piece of paper. That is subject to a subsisting statutory copyright.

Mr. FRANK. Well, you did not answer my question. Your whole book, frankly, is less relevant.

What about someone who has prepared work for commercial purposes but have not yet marketed—is not sure he or she is going to.

Why do you make them unprotected? Is there no way to protect your child's kindergarten drawing without doing that?

Mr. NIMMER. Congressman, I fully appreciate that there are many opportunities for fixes, and this would be one of them.

As the Chairman asked about——

Mr. FRANK. Answer my question, Mr. Nimmer.

Mr. NIMMER. I would like to.

Mr. FRANK. But you are not.

Do you really want commercially—I mean why only commercially marketed?

Mr. NIMMER. It is a legitimate point. If a work has been registered and yet it has not been commercially exploited yet, to come up with another scenario, I fully agree that that could be within a rational bill. And we are most open to working with the Committee and with our colleague.

Mr. FRANK. I know it could be. Granted, it could be.

I guess I am telling you this. Here is my problem. You come in and you say, "There is a problem here," but you then take a very grudging approach to it, and I want to be explicit to everybody here because people are going to—you know, there is a question of your credibility.

If you come in and say, "Yeah. There is a problem," and then you give a very grudging fix, I mean it was just an opening negotiating position, do not come to me with an opening negotiating position. I have not got time for that.

I mean you have got a proposal which you defend which has huge loopholes. And you point to the problems with other people's, but then you come in with your own.

That is not a good use of everybody's time. So I do not understand why would you—why did you restrict it that way?

Mr. NIMMER. Because of what I said before, that the copyright laws extend to so many millions of works that——

Mr. FRANK. And you are incapable of—were you incapable of a fix short of that?

Mr. NIMMER. To be honest, I did not focus on that particular situation.

Mr. FRANK. Very well. The other one, then—so you would not object to our tightening that substantially?

Mr. NIMMER. Correct.

Mr. FRANK. Well, loosening it, I guess I would say.

Certain criterias, and here is my other problem, I do not want this to expand the liability of the service provider, but neither do I want it to contract it, and it does seem to me you are contracting it because your plan—and I assume I am reading this right—whoever places the material on.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 160 1999

So is it your intention from this language, and would it not be a threat to immunize the provider, no matter how much collaboration, knowledge, et cetera there was?

Mr. NIMMER. Under this language, yes. But somebody——

Mr. FRANK. Why would you——

Mr. NIMMER [continuing]. Aiding and abetting liability. To the extent that——

Mr. FRANK. Yes, but these are what you are proposing and I do not understand why——

Once again, you are arguing your point badly. And please do not—I would just ask everybody, please do not do that.

I mean you have got in here, it has got to be commercially marketed and it is a total immunization from the provider in any case.

You did not subjectively add something for aiding and abetting.

Now the people who put the word forward do not need to do aiding and abetting because they have not excluded people this way.

So your proposal would totally immunize the provider, even where there was a degree of collaboration. And, again, it is just not a good use of everybody's time.

Mr. NIMMER. I apologize for not anticipating all of these eventualities, but I would be happy to work——

Mr. FRANK. Mr. Nimmer, these are little nit things and you know more about this subject than I do. So the notion that I was able somehow to divine, on reading your statement this morning, things that did not occur to you makes me skeptical.

I think—I am going to ask you to redraft this if you want it seriously considered because I do not want to extent liability to the providers. I want to keep the providers free. I do not want anybody getting an incentive to censure.

But I would need you to give me something other than this, if you want it to be a starting point for the Bill.

Thank you, Mr. Chairman.

Mr. PEASE. The gentle lady from California is recognized for five minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. Nimmer, looking at the proposal that just was reviewed by Mr. Frank, in addition to making sure that we tighten this measure so that it would include material that is intended to be marketed, but not yet marketed, I do not see room for fair use under the Fair Use Doctrine here.

Could you comment on that?

Mr. NIMMER. Yes, Congresswoman. I share your sensitivity that fair use needs to be jealously guarded in the online environment.

You have pointed out a useful feature to me, as I think about it, and this is another matter that needs to be thought about because the precise way the language reads does need more sensitivity to fair use. So I appreciate the question.

Ms. LOFGREN. OK. For Mr. Sherman and Mr. Attaway, it occurs to me that, and clearly, you are right. I mean your industries have been protected to some extent because of bandwidth restrictions.

But as we look forward, that will change. It is changing rapidly, and we do need to address those issues. I do not think there is any disagreement here.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 161 1999

But I also believe that oftentimes, the challenges posed by technology are quickly mediated by technology. And I am interested in how far along you are in pursuing the technological protections that are available to content providers through watermarking, and then also through some of the new variations on encryption that basically will protect your products if you choose to utilize them.

Mr. ATTAWAY. Congresswoman, our top priority is to use technology to help ourselves—to protect ourselves against piracy.

But, as good as technology is and will become, it is never perfect, and for every technological development that protects copyrighted material, the bad guys come up with a technological development that defeats it.

Ms. LOFGREN. Oh, it is constant. Yes. I understand. It will continue in that mode.

Mr. ATTAWAY. And that is why legislation addressing anti-circumvention——

Ms. LOFGREN. Well, I am not suggesting——

Mr. ATTAWAY [continuing]. Is so critical.

Ms. LOFGREN [continuing]. That we will not have legislation. We will have lots of hearings and discussion. But since you are here, I want to know how far along you are in helping yourself in that way.

Mr. ATTAWAY. It is a top priority. Personally, I have devoted my life in the last year to this effort, and I will continue to do so.

Mr. SHERMAN. And it is certainly very top priority for the recording industry, as well. We are pursuing a number of different strategies.

Bear in mind, however, that no matter what we do with respect to the protection of material in the future, we have out there some four billion CD's, each of which can be uploaded to the Internet and disseminated worldwide. And it becomes a special challenge to figure out how you are going to protect those on the Internet. And that is why we feel like we are going to need the cooperation of the network services that disseminate those transmissions. That is why we need a cooperative solution technologically, as well.

Ms. LOFGREN. I think it would be very helpful, frankly, for the principals in the various sectors of the economy that have an interest in this to spend some quiet time talking with each other because I believe, ultimately the way your product is delivered is going to be fundamentally changed.

Why would anyone bother to go to a record store? There will not be record stores because they will be superfluous. Just as Amazon.Com is going to have a huge impact on Barnes and Noble, the Internet is going to be the primary delivery source of your product, and your products, Mr. Attaway. And so it is definitely in your interest that we do nothing to impair the growth and productivity of the Internet, because you are going to rely on it.

I want to protect intellectual property, but we also need to protect the Internet. And so I think there are some very easy fixes for some of these things that will do—accomplish both. But I think our country will be better off if, after this hearing, you all go out and have lunch and sort through some of these issues. And I would like to make that suggestion.

Mr. NIMMER. Mr. Chairman, may I add a brief note on that?

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 162 1999

I would like to grasp the hand that Mr. Sherman offers to speak to the networks because we, at the USTA, believe that we also would like to be part of the solution.

From the Adobe spokesman earlier, we learned that not even the content owners can police all of their copyrighted materials on the network.

We believe that we are not situated to police those. However, we would like to work assiduously with the content owners to develop the best techniques that we can to regulate them.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. PEASE. Thank you.

The gentleman from Massachusetts is recognized for five minutes.

Mr. DELAHUNT. Thank you. I would just associate myself with the remarks of Representative Lofgren. I am sure after listening to her, you are fully aware now that she is the tekkie on this particular Subcommittee, and we look to her for counsel on that regard, because she does have the best understanding of the technology.

But I was going to pose that question. I think it really makes sense for you to take the time to sit down and to explore ways of protection.

Also, that if there should be at some point in time a criminal prosecution, it is very important in terms of the rules of evidence to have a—to provide a—to provide evidence to the prosecuting agency that deals with all of the issues surrounding chain of custody, et cetera, et cetera.

And so I mean I think that it can be done, and I have confidence that, you know, that can be met—the technology in the end is going to hopefully be the answer to this issue of piracy.

And I also associate myself with the remarks of my friend from Massachusetts, Mr. Frank, that was directed to Mr. Nimmer about sitting down in good faith, and not in a negotiating/adversarial way. But, you know, we are closer to this.

I have a sense that this Subcommittee will and should act expeditiously to move this along. So sit down, get some language.

I honestly do not believe that the Department of Justice is going to indict any member of the United States Telephone Association. That is not really the intent. That is not the spirit within which people are operating.

We are not looking for arcane nuances and in delving into high-visibility chases in—other than those little criminal syndicates.

The admonition that he did say is to not try to expand. Do not try to contract. I do not think you need very much work at all, but if it allays some, what I consider unjustified concerns on the part of your clients, I think it can be done readily.

Mr. NIMMER. Mr. Delahunt, I believe you mentioned that you, too, were a former Federal prosecutor. We saw——

Mr. DELAHUNT. A state prosecutor.

Mr. NIMMER. Oh, thank you.

We saw before what happens when a war is declared. When the war on drugs is declared, the line shifts such that 15 years later, it exists in a place where no one could have possibly conceived it being 15 years earlier.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 163 1999

If there is a war on intellectual property theft today, I applaud it, but I think it is essential at the outset to draw the line in exactly the proper place. And that is the spirit that brings USTA here.

Mr. FRANK. And I am confident that you can do that, Mr. Nimmer.

Mr. ATTAWAY. Congressman Delahunt, if I may comment on what you said, and also on Congresswoman's Lofgren's comments.

I represent an industry that does not always grasp new technology and the opportunity that it provides with the vigor that we possiblly could have and should have.

Let me assure you that we look at the Internet as an opportunity, not a threat. Every single one of the companies I represent is in the online access business. It is definitely an opportunity. We do not want to kill the Internet. We want the Internet to be a new marketplace for us.

Mr. SHERMAN. And certainly the same is true for the recording industry.

Mr. PEASE. Thank you, Mr. Delahunt.

I know we have asked you to be quick in your testimony, but I do not want you to leave feeling that you did not have the opportunity to at least follow up on a couple of points that each of you made.

Mr. Sherman, you mentioned that you had a concern about the increase in the threshold to $5,000 before prosecution would take place.

Do you have anything further you want to add on that so we can make sure we have it before us?

Mr. SHERMAN. Well, let me just explain that briefly.

It is a difficult thing to pull together a case for a civil infringement or a criminal infringement. You need proof of the copyright registration and you need the title issues that Mr. Delahunt was referring to, and you need affidavits. And you need that for each and every copyrighted work that is part of the indictment.

Now when you have a situation where you have millions of dollars of units, the U.S. Attorney will still only plead the $2500 amount because the U.S. Attorney is trying to avoid the amount of work that would be required to do the entire case. So there is still a lot of work to do the $2500.

Well, to do 5,000, you will have to do twice the amount of work, twice the number of affidavits, and so on and so forth.

More uniquely in the Internet environment, you do not have multiple copies of products being made available to the public. It is not a question of one Michael Jackson album being reproduced a thousand times and put out on the street.

One copy is made and put on a server for everybody to come and take one. So you have basically a singles market, and you would have to then have something like 3300 singles, which means 3300 separate copyrights, in order to meet that minimum standard.

That is just difficult to do because of capacity problems on the servers. We have found sites with a thousand full-length sound recordings, but not 3300.

So that is why it has this unintended consequence of making prosecution more difficult.

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 164 1999

Mr. PEASE. Thank you, and thank you for bringing that to us.

And, Mr. Attaway, you mentioned, also, I think a request that the definition of the term, "financial gain," as proposed, be amended, to include not only receipt of something of value, but the expectation?

Mr. ATTAWAY. Yes, sir.

Mr. PEASE. Can you elaborate a bit on that for us?

Mr. ATTAWAY. The problem is that in some cases—like when we raid a video lab that has hundreds, maybe thousands of copies of pirated movies sitting in a warehouse—it is difficult or maybe even impossible to prove that money has actually changed hands, although there is clearly the expectation of receipt of money. And the courts have interpreted existing law to include expectation of receipt.

And we just would feel more comfortable if the NET Bill was amended to make that explicit.

Mr. PEASE. And you could provide us, I am sure, some of the decisions where that definition has been set forth so that we can make sure we harmonize legislation?

Mr. ATTAWAY. Yes, sir. I would be glad to do that.

Mr. PEASE. OK.

Mr. DELAHUNT. It would be presumably as an attempt to, under the attempt provision.

Mr. PEASE. All right. Thank you very much.

At the risk of encountering a hostile audience, I will give opportunity for either of the members of the Committee to ask more questions at this time or pass.

Ms. LOFGREN. I think this has been very helpful, and I know we are going to have additional hearings and witnesses.

We need to do something in this area, but we need to do the right thing that is carefully crafted and balanced and avoids unintended consequences.

And I presume we will have some of the Yahoos of the world and others coming in to give their perspective. And I think all of that is going to aid us greatly in coming up with, hopefully, a very good bill that we will move forward on a bipartisan basis.

So I do not have additional questions. This has been helpful and I hope that you all go out and have lunch together and kick this around.

Mr. DELAHUNT. I thank the panel. I thank the previous panels. It was very informative.

Mr. PEASE. This concludes our hearing. I want to thank the witnesses for their testimony, the Subcommittee for their participation.

The record will remain open for one week.

The Subcommittee stands adjourned.

[Whereupon, at 12:33 p.m., the Subcommittee adjourned.]

○

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 165 1999

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress 166 1999

Document No. 5

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [i] 1999

HeinOnline -- 1 William H. Manz, Federal Copyright Law: The Legislative Histories of the Major Enactments of the 105th Congress [ii] 1999