

PANEL III: Implications of Enforcing the
Digital Millennium Copyright Act:
A Case Study, Focusing on *United States
v. Sklyarov*

Facilitator: Edward Burke*

Panelists: Joseph Burton**
Mark Allen Cohen***
Jesse Feder****
Robin Gross*****
Bruce Lehman*****
Eric Smith*****

MS. SUHL: Good afternoon. I am Natalie Suhl, Managing Editor of the *Fordham Intellectual Property, Media & Entertainment Law Journal*. I would like to present Edward Burke of Weil, Gotshal & Manges, who will be facilitating Panel 3, entitled “Implications of Enforcing the Digital Millennium Copyright Act.”¹ It is a case study

* Associate, Weil, Gotshal & Manges, LLP. State University of New York at Binghamton, B.A.; Fordham University School of Law, J.D.

** Partner, Duane, Morris & Heckscher. University of Dayton; Northeastern University School of Law, J.D.

*** Attorney-Advisor, Office of Legislative and International Affairs, United States Patent and Trademark Office.

**** Acting Associate Register for Policy and international Affairs, United States Copyright Office. Yale University, B.A.; Columbia University School of Law, J.D.

***** Attorney, Electronic Frontier Foundation. Michigan State University, B.A.; Santa Clara University, J.D.

***** President, International Intellectual Property Institute. University of Wisconsin, B.A.; University of Wisconsin, J.D.

***** Partner, Smith & Metalitz LLP. Stanford University, B.A.; University of California at Berkeley (Boalt Hall), J.D.

¹ The Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. §§ 512, 1201-05, 1301-22 (West Supp. 2000) and 24 U.S.C.A. § 4001 (West Supp. 2000)) [hereinafter *DMCA*].

focusing on the first criminal case under this Act, *United States v. Sklyarov*.²

MR. BURKE: Thank you. Good afternoon.

I want to first congratulate the *Journal*. They have brought together an amazing panel. I think before you leave today, the people you are going to hear from are very much at the center of the issues surrounding the Digital Millennium Copyright Act (hereinafter "DMCA"), including the important litigation that has arisen from it.

I am going to introduce the panel, and this is the order in which they will be speaking: first, Jesse Feder, who is the Acting Associate Register for Policy and International Affairs with the U.S. Copyright Office;³ after Jesse will be Joseph Burton, the attorney for Mr. Sklyarov, who is a partner with the firm of Duane, Morris & Heckscher;⁴ third will be Bruce Lehman, who is the President of the International Intellectual Property Institute and someone who played a central role in the creation of the DMCA,⁵ after that is Robin Gross, who is an intellectual property attorney with the Electronic Frontier Foundation, an organization that has been very much in the forefront of advocating with respect to the issues in the *Sklyarov*

² See *United States v. Dmitry Sklyarov*, Criminal No. 5-01-257P (N.D. Cal. filed 2001) (charging defendant for being in violation of Title 17 U.S.C. § 1201(b)(1)(A) and 18 U.S.C. § 2), available at http://www.eff.org/IP/DMCA/US_v_Sklyarov/20010707_complaint.html [hereinafter *Sklyarov Complaint*].

Significant developments in the case occurred during the editing of this symposium. On December 13, 2001, the U.S. Attorney's Office for the Northern District of California issued a press release which announced that Dmitry Sklyarov entered into an agreement with the United States, admitted his conduct in a hearing before U.S. District Judge Whyte in San Jose Federal Court, and agreed to cooperate with the United States in its ongoing prosecution of Mr. Sklyarov's former employer, ElcomSoft Co., Ltd. U.S. Attorney (N.D. Cal.) Press Release On Dropping Charges Against Dmitry Sklyarov (Dec. 13, 2001), available at http://www.eff.org/Cases/US_v_Elcom/20011213_usatty_pr.html (last visited Mar. 13, 2002).

³ The views expressed by Jesse Feder are individual opinions and not necessarily those of the U.S. Copyright Office. The U.S. Copyright Office Web site may be accessed at <http://www.loc.gov/copyright/> (last visited Feb. 16, 2002).

⁴ Duane, Morris & Heckscher, LLP's Web site may be accessed at <http://www.duanemorris.com/> (last visited Feb. 16, 2002).

⁵ The International Intellectual Property Institute Web site may be accessed at <http://www.iipi.org/>.

case;⁶ and after Robin will be Eric Smith, who is a Partner in the firm of Smith & Metalitz and President of the International Intellectual Property Alliance;⁷ and then weighing in will be Mark Cohen, who is an Attorney-Advisor with the U.S. Patent and Trademark Office.⁸

Welcome.

I am going to give a couple of comments to try and set up the issues that will be discussed today. One of the sources that I have relied upon is the complaint filed by the Government, so please keep in mind that these are allegations, not facts. In the event that I do not speak correctly, I am sure my colleagues on the panel will correct any lapses.

First of all, the indictment,⁹ filed on August 28th by the United States Government in the Northern District of California, was done so under what are called the “anti-trafficking provisions” of the DMCA.¹⁰ The indictment includes five counts against both Mr. Sklyarov and his employer, a Russian company called ElcomSoft Ltd.¹¹

The indictment raises the following legal theories: first, conspiracy; second, trafficking for gain in technology primarily designed to circumvent technical measures that protect the rights of a copyright owner, also trafficking for gain in technology marketed for

⁶ The Electronic Frontier Foundation Web site may be accessed at <http://www.eff.org/>.

⁷ Smith & Metalitz, LLP, specializes in global and domestic copyright, trade, trademark, entertainment and information law and policy advocacy. The views expressed are individual opinions and not necessarily those of IIPA. IIPA is a coalition of six trade associations representing over 1,100 U.S. companies producing and distributing copyrighted materials domestically and globally.

⁸ The views expressed by Mark Cohen are individual opinions and not necessarily those of the U.S. Patent and Trademark Office. The U.S. Patent and Trademark Office Web site may be accessed at <http://www.uspto.gov> (last visited Feb. 16, 2002).

⁹ See *United States v. Dmitry Sklyarov*, Criminal No. 5-01-257P (N.D. Cal. filed 2001) (indictment of Dmitry Sklyarov and Elcomsoft, Ltd.), available at http://www.eff.org/IP/DRM/DMCA/US_v_Sklyarov/20010828_sklyarov_elcomsoft_indictment.pdf [hereinafter *Sklyarov Indictment*].

¹⁰ 17 U.S.C.A. §§ 512, 1201-05, 1301-22 (West Supp. 2000); 24 U.S.C.A. § 4001 (West Supp. 2000) [hereinafter *DMCA Anti-Trafficking Provisions*].

¹¹ *Sklyarov Indictment*, *supra* note 9; Elcomsoft's Web site may be accessed at <http://www.elcomsoft.com/>.

use in circumventing technological measures that protect the rights of a copyright owner; and third, aiding and abetting.¹²

The penalties under this statute are quite severe. I am sure Mr. Burton will discuss these further. Every report I have read comes out differently as to how significant the financial penalties can be, and I hope that he can elucidate that. The statute is not entirely clear as to what the potential penalties are.¹³

Here is a thumbnail sketch of the facts. As you know, the case is extremely controversial. It has generated a tremendous amount of press. It is the first significant criminal prosecution under the DMCA. I think this case will raise important issues about the scope and reach of the statute.

The Government's complaint states that in June of 2001, the FBI was contacted by Adobe.¹⁴ Adobe makes a product called the Adobe eBook Reader.¹⁵ After the eBook Reader is downloaded onto an individual's computer, the user can contact e-book sellers, such as amazon.com or barnesandnoble.com, and purchase book titles in electronic format, which are known as e-books.¹⁶ There may be others, but I think that there are two other products on the market. One is produced by Microsoft and the other by Gemstar.¹⁷ The

¹² *Sklyarov Indictment*, *supra* note 9.

¹³ *See DMCA Anti-Trafficking Provisions*, *supra* note 10.

¹⁴ *See Sklyarov Complaint*, *supra* note 2.

¹⁵ *See* Adobe Web site, Adobe Acrobat eBook Reader 2.2, at <http://www.adobe.com/products/ebookreader/main.html>. Adobe Acrobat eBook Reader "enables you to read high-fidelity eBooks on your notebook or desktop computer without the need for special hardware." *Id.*

¹⁶ Customers visiting Amazon.com's eBooks store can download the Acrobat eBook Reader free of charge and choose from a vast selection of Adobe PDF titles. *See* Press Release, Adobe and Amazon.com to Extend Availability of Adobe Acrobat eBook Reader and eBook Titles Worldwide (Apr. 10, 2001), at <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200104/20010410amazon.html>.

¹⁷ Microsoft Reader with ClearType "gives book lovers powerful digital advantages like integrated dictionary support and electronic annotations, while honoring the best traditions of typography to ensure proper kerning and leading, correct margins, and line justification, to name a few. The software builds the eBook, page-by-page, according to your preferences to suit the device you're using." *See* Microsoft Web site, The Microsoft eBooks Story, at <http://www.microsoft.com/reader/info.asp>. The Gemstar eBook is the only complete electronic reading solution providing you instant access to thousands of books, as well as newspapers and periodicals. *See* Gemstar Web site, Welcome to Gemstar eBook, at

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 809

computer user may only open and view the encrypted book on the specific computer that the user has used to receive the e-book, which, as you can imagine, is an issue of tremendous controversy in the case.

When the e-book is purchased for viewing in the Adobe eBook Reader format that was sold by a publisher or distributor, those companies could authorize or limit the purchaser's ability to copy, distribute, print, or have the text read audibly by the computer. Again, these are further significant issues of contention in this case.

The complaint alleges that ElcomSoft was selling a key over the Internet in the form of a software program that unlocks the protections created by the Adobe eBook Reader.¹⁸ The unlocking key is available for purchase from a Web site in the State of Washington. ElcomSoft calls this key the "Advanced eBook Processor."¹⁹ Using the ElcomSoft key, the decrypted file can be opened in any PDF viewer, for example the Adobe Acrobat Reader, without any restrictions. Therefore, the user can edit, copy, print or take advantage of certain annotations from e-books, which can alternatively be restricted by the Adobe product.

Now I want to quote from the complaint. The complaint states as follows: "The real damage done by the ElcomSoft program is that it creates a 'naked file' that enables anyone to read the e-book on any computer without paying a fee to the book seller. Only one legitimate copy of the encrypted book needs to be purchased originally, and after the protections are stripped through usage of the ElcomSoft program, there are no restrictions and the e-book can be duplicated freely and made available for usage on any computer."²⁰

On June 26th, Adobe purchased the program from ElcomSoft, through a U.S.-based company, for \$99.²¹ That company is called Register Now in the State of Washington.²² The key was sent to

<http://www.gemstar-ebook.com/cgi-bin/WebObjects/eBookstore>.

¹⁸ See *Sklyarov Complaint*, *supra* note 2.

¹⁹ See Adobe Web site, Description of Advanced eBook Processor, at <http://www.adobe.com/products/ebookreader/main.html>.

²⁰ See *Sklyarov Complaint*, *supra* note 2.

²¹ *Id.*

²² The Register Now Web site may be accessed at <http://www.regnow.com>.

Adobe in San Jose, California. You should note that ElcomSoft does allow a free download of a demo, which would allow a user to look at 10 percent of an e-book, but if you want to be able to look at the entire book, you have to pay the \$99 fee.²³

As far as I am aware from reading the press, there have been only a few copies of the ElcomSoft key sold, perhaps under ten.²⁴ I am not sure of the exact number, but it appears to be a minimal number.

The complaint further alleges that the opening screen of the ElcomSoft software purchased allegedly shows that a person named Dmitry Sklyarov is the copyright holder of the ElcomSoft program.²⁵ News accounts have identified Sklyarov as the creator of the algorithms underlying the ElcomSoft software.²⁶

Sklyarov was scheduled to speak at the Def Con-9 Conference in Las Vegas in mid-July.²⁷ The Def Con Web site stated that he was scheduled to speak about security aspects of electronic books and give a demonstration of how weak those systems are.²⁸ Sklyarov was arrested at the Def Con convention and spent time in jail in Nevada.²⁹ He was then transferred to California, where eventually he was released on \$50,000 bail.³⁰ The Government has taken his

²³ See Elcomsoft Web site, at <http://www.elcomsoft.com> (last visited Feb. 2, 2002).

²⁴ See Jennifer Lee, *Man Denies Digital in First Case Under '98 Act*, N.Y. TIMES, Aug. 31, 2001, at C3 (stating that "Mr. Katalov [President of Elcomsoft] said that the Advanced eBook Processor . . . probably sold fewer than 10 copies before it was pulled, under pressure from Adobe Systems.").

²⁵ See *Sklyarov Complaint*, *supra* note 2.

²⁶ See Lee, *supra* note 24 (noting that "[Mr. Sklyarov] was one of three programmers who worked on the Advance eBook Processor and was originally listed as the holder of the copyright").

²⁷ Bill McCarthy, *Land of the Free? Service Providers Should Beware as Copyright Problems Loom*, AMERICA'S NETWORK, Sept. 15, 2001. Def Con is a major annual technical conference dealing in part with underground Internet security issues. Def Con attracts about 4,000 people per year. It has been held for the last nine years. *Id.* The Def Con Web site may be accessed at <http://www.defcon.org/>.

²⁸ Sklyarov's presentation was announced on the Def Con Web site, at <http://www.defcon.org/>.

²⁹ See Lee, *supra* note 24.

²⁹ See Press Release, Electronic Frontier Foundation, Russian Programmer and Company Case Continued: New Date for Hearing, (Nov. 26, 2001), available at http://www.eff.org/IP/DMCA/US_v_Sklyarov/20010904_eff_sklyarov_elcom_pr.html.

³⁰ See *id.*

passport and, as far as I understand, his ability to travel has been restricted by the Government.

Sklyarov is a twenty-six-year-old computer programmer who was working for ElcomSoft while finishing his Ph.D.³¹ He has two young children.³² He has not been back to Russia since he was arrested.³³ According to *Time* magazine, what Sklyarov did is legal in the rest of the world and, until the DMCA, was legal in the United States as well.³⁴

The case has raised a firestorm of controversy, huge protests against Adobe, so much so that Adobe released a statement saying that the prosecution of Sklyarov was not in the best interests of the industry.³⁵ Adobe now says that it did not ask the Government to arrest Sklyarov, but rather, made a more general complaint against the company.³⁶ The U.S. Attorney has not commented.

This case sharply focuses the arguments on both sides of the issue of the DMCA. On the one hand, publishers are legitimately concerned that software like that sold by ElcomSoft could completely eliminate the market for e-books. If copies of e-books can be made and distributed over the Internet, only one book would have to be sold and millions of copies theoretically could be made and distributed. On the other side of the argument, scholars and lawyers argue that the DMCA gives copyright owners broad rights that they never had before and that technology, rather than copyright law, in theory is driving the development of the law.

³¹ See Carrie Kirby, *Sklyarov Denies He's a Hacker*, S.F. CHRON., Aug. 31, 2001, at B1.

³² *Id.*

³³ *Id.*

³⁴ See Chris Taylor, *Throwing the E-Book at Him; A Programmer is Prosecuted for Enabling Users to Break the Security in Reader Software*, TIME, Aug. 20, 2001, at 62.

³⁵ See James Connell, *Tech Brief: Adobe Seeks Russian's Release*, INT'L HERALD TRIB., July 25, 2001, at 11.

³⁶ See Adobe Web site, Adobe FAQ: ElcomSoft Legal Background, at <http://www.adobe.com/aboutadobe/pressroom/pressreleases/200108/elcomsoftqa.html>.

Lawrence Lessig, who is a Professor of Law at Stanford University and founder of Stanford's Center for Internet and Society, recently wrote an op ed piece in *The New York Times*. Here is what he says: "The DMCA is a law which protects software which protects copyright."³⁷ The problem, as Lessig sees it, is that technologies that protect copyrighted materials are never as subtle as the law of copyright. For example, copyright law permits fair use; technology may not do so. Copyright law also protects only for a limited amount of time; technologies do not necessarily have any such time limitation. Lessig states that technology protects more broadly than copyright law does, and I think that that is an important issue that will be raised in this case. Lessig concludes: "The relevant protection for copyrighted material becomes as the technology says, not as the copyright law requires."³⁸

So that is essentially the framework for today's debate.

I want to read to you the statutory language. Jesse is going to talk more about the DMCA, but I just want to read you what the statute provides. Section 1201(b)(1) provides:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work, or a portion thereof, . . . or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.³⁹

³⁷ Lawrence Lessig, *Jail Time in the Digital Age*, N.Y. TIMES, July 30, 2001, at A17.

³⁸ *Id.*

³⁹ See DMCA, *supra* note 1, § 1201(b)(1).

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 813

I am now going to turn to the panelists. Each of the panelists will be speaking for approximately ten minutes. We will then have some debate among ourselves and then open it up to the audience for questions.

I will turn now to Jesse Feder.

MR. FEDER: Thank you.

First of all, I just want to say that my office does not have any position as such on the *Sklyarov* case.⁴⁰ We are not involved in the enforcement of the copyright. That is not our role. We were, however, very deeply involved in drafting the DMCA, particularly during the period after the Administration submitted it to Congress through to its final passage.

Let's talk a little bit about where the DMCA came from. In 1976, when the present Copyright Law was enacted, the big technological concerns on people's minds were the impact of photocopying and the impact of cable television.⁴¹ Digital networks, digital technologies, were not really forefront in the thinking of anybody back in 1976, but they certainly came to be at the forefront of thinking as time went on.

Digital technology makes copying and distributing protected works a trivial matter. In order to make a complete copy of a book, I have to spend hours in front of a photocopier, copying it page by page, or two pages at a time. To make a complete copy of an electronic book, I have to click a mouse a couple of times and I have a copy. To distribute that copy I need only put it on my Web page, and within a matter of hours thousands of people can download it, they can put it on their own Web pages, and within hours thousands of people can download it from those pages, and its presence on the Internet spreads geometrically.

So by the mid-to-late-1990s, when these issues came into focus, it was very clear that the balance that had been struck in 1976, based as it was on the state of technology at that time, had shifted

⁴⁰ See *Sklyarov Complaint*, *supra* note 2.

⁴¹ See H.R. REP. NO. 94-1476 (1976), 1976 WL 14045 (Leg. Hist.).

dramatically in favor of those who would use copyrighted works without permission. The purpose of legislation at that time was to redress that balance, to make it as difficult to engage in unauthorized uses of copyrighted works in the digital realm as it was in the analog realm, and the means of doing this was employing technological protection measures.⁴²

The problem, of course, is that technological protection measures, which are very often quite expensive and difficult to produce, can be hacked and you get involved in an arms race. When we talk about hacking a technological protection measure, we are not talking about really the equivalent of going and picking a lock. We are talking about going and kicking in the door, and kicking in the door of every copy of every work that is protected by that particular technological measure once the cat is out of the bag. So, from a policy standpoint, it appears to make perfect sense to create legal prohibitions on that kind of activity, not only in the United States. This is not just a U.S. issue but an international one as well.

The obligation to create prohibitions on circumvention of technological measures is in a treaty, in the WIPO Copyright Treaty,⁴³ and also in the WIPO Performances and Phonograms Treaty.⁴⁴ These treaties will in most nations go into force sometime either near the end of this year or early next year. There will be at that point at least thirty countries on each treaty for which these obligations are binding.

So the fact that we were first across the line in implementing this obligation does not mean that these are not legal provisions that we will be seeing in other countries' laws. The fact is other countries are going to have to implement these provisions in some way. Now, the Treaty leaves some room for maneuver, but the standard is that

⁴² See S. REP. NO. 190 (1998), 1998 WL 239623 (Leg. Hist.).

⁴³ World Intellectual Property Organization Copyright Treaty, adopted by Diplomatic Conference at Geneva, Dec. 20, 1996, 36 I.L.M. 65 (1997) [hereinafter *WIPO Copyright Treaty*], available at <http://www.wipo.org/treaties/ip/copyright/index.html>.

⁴⁴ World Intellectual Property Organization Performances and Phonograms Treaty art. 6 adopted by Diplomatic Conference at Geneva, Dec. 20, 1996, 36 I.L.M. 76 (1997) [hereinafter *WIPO Performances and Phonograms Treaty*], available at <http://www.wipo.org/treaties/ip/performances/index.html>.

there must be adequate legal protection and effective legal remedies against circumvention.⁴⁵ We did a lot of thinking in the United States about what constitutes adequate legal protection and effective legal remedies, and what we came up with is what is in the DMCA.⁴⁶ There are essentially three prohibitions. The first one is a prohibition on the conduct of circumventing access control measures.⁴⁷ The second is a prohibition on manufacturing, trafficking, importing, et cetera, of technologies or devices, including software, that circumvent access control measures.⁴⁸ The third, which is the one involved in this case, is a prohibition on, again, manufacturing, trafficking in, importing of technologies, devices, including software, that circumvent what we refer to as 'copy control protections.'⁴⁹ That is just a shorthand for a protection that prevents you or inhibits you from engaging in any of the exclusive rights of an author without authorization. So that is the law that was created.

The remedies are two-fold. There are civil remedies under the law,⁵⁰ which can be very effective if you can get your hands on the defendant, but if the defendant is acting abroad and trafficking in these materials over the Internet, it becomes very difficult to apply civil remedies. So, in addition, there are criminal provisions, and the maximum penalties under those provisions are pretty severe.⁵¹ I will let Mr. Sklyarov's counsel go into precisely what those criminal penalties are.

But it is important to note that, in addition to the basic elements of the prohibition, the government must also demonstrate that the conduct was done willfully and for purposes of commercial advantage of private financial gain.⁵² So we are talking not merely about violation of the prohibition, but a prohibition that is done

⁴⁵ See *id.*; see also *WIPO Copyright Treaty*, *supra* note 43.

⁴⁶ See *DMCA*, *supra* note 1, § 1201.

⁴⁷ See *id.* § 1201(a)(1).

⁴⁸ See *id.* § 1201(a)(2)(A).

⁴⁹ See *id.* § 1201(b)(1)(A).

⁵⁰ See *id.* § 1203.

⁵¹ See *DMCA*, *supra* note 1, § 1204. The criminal penalties under the DMCA are a maximum of five years in prison and/or a fine up to \$500,000 for the first offense and a maximum of ten years in prison and/or a fine up to \$1,000,000 for any subsequent offense.

Id.

⁵² See *id.* § 1204(a).

willfully, with a profit motive.⁵³ That is what criminal penalties attach to under the law.

Before I finish, I just want to mention a couple of things that I have heard about that appear to be incorrect in talking about this case. First of all, this is not a case about encryption research. It does not appear to me, at least from the facts that I am aware of about this case, that the facts bear out that this was a research project of some sort. This was a commercial endeavor. This is not a prosecution based on the circumvention of a copy control technology. In fact, circumvention of a copy control technology is not prohibited under the law.⁵⁴ This is not something that flowed out of the defendant's statements at the Def Con-9 conference. He was not arrested for what he said there. He was arrested for trafficking in circumvention devices. This is not a case about writing a computer program in Russia, where writing that program would be legal. He has been indicted under the trafficking provisions, selling it in the United States.⁵⁵ Now, it is not clear to me at all whether the government will be able to prove that based on the facts in this case, but that is what he was indicted for. He was not indicted for writing the program in Russia.

⁵³ *See id.*

⁵⁴ *See id.* § 1201(a)(1).

⁵⁵ *See Sklyarov Complaint, supra* note 2.

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 817

And finally, this is not a case about fair use.⁵⁶ First of all, I think it stretches credulity to say that a program that was marketed for \$99 was being marketed for making fair-use excerpts from \$12 e-books. Second of all, you do not need to make a perfect digital reproduction of an entire work in order to engage in fair use. In 1976, you could not do that. You could excerpt from it, you could write it down, you could photocopy some pages, you could take some screen shots on your computer, but there is no compelling reason under the fair use doctrine that you should have to make a complete digital reproduction of an entire work stripped of all of the technological protection measures.

And finally, I would just say that the sky is not falling. This is a single prosecution. In the three years that this law has been in effect, this is the first prosecution under this law. We will have to see how it plays out. But before we even get to a conviction in this case, the government has many elements that it needs to prove. But I would submit to you that if the government does prove those elements, if the government does prove that there has been trafficking and that the defendant has engaged in that, and that this conduct was done globally and for purpose of commercial advantage or private financial gain, that this is not some sort of aberration, but this comes very close to the kind of conduct that Congress intended to criminalize when it enacted the DMCA in 1998.⁵⁷

⁵⁶ CRAIG JOYCE, WILLIAM PATRY, MARSHALL LEAFFER & PETER JASZI, COPYRIGHT LAW 807-8 (5th ed. 2000) (citing the Copyright Register's 1961 Report, at 24) [hereinafter *Definition of Fair Use*]. The fair use doctrine provides an affirmative defense after the plaintiff in a traditional copyright action has made a prima facie case. Courts view certain uses of copyrighted works as fair, non-infringing uses of the works. These include, but are not limited to, "quotation[s] of excerpts in a review or criticism for purposes of illustration or comment; quotation of short passages in a scholarly or technical work, for illustration or clarification of the author's observations; use in a parody of some of the content of the work parodied; or a summary of an address or article, with brief quotations, in a news report." These examples fall under the doctrine as codified in 17 U.S.C. § 107. *Id.*; see also 17 U.S.C. § 107 (1988). This Copyright Act sets forth four factors that courts use in determining whether a fair use defense protects the alleged infringer: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. *Id.*

⁵⁷ See generally *DMCA*, *supra* note 1.

MR. BURKE: We are next going to hear from Joe Burton, who is Mr. Sklyarov's attorney.

MR. BURTON: I am going to stand because I cannot, being a trial attorney, talk sitting down, so you will have to excuse me, but I have to stand. The sky falling? Well, you know, the sky is not falling if you are not the defendant who is facing five years and a \$250,000 fine. You know, maybe to a lot of people that does not seem like the sky is falling, but it seems to me, if I were thinking about spending five years in jail, or the potential of that, it would.

Now, let me say, because I don't want to mislead anybody, the five years and the \$250,000 is the maximum penalty that is allowed by the statute.⁵⁸ Because of another aberration—and when I use the term 'aberration' I am in good company, because not only defense counsel say it, but lots of judges in the federal court will say it. But because of another aberration, called the Sentencing Guidelines, which we do not have time to go into (we could do a whole symposium on the Federal Sentencing Guidelines) but because of the Federal Sentencing Guidelines, in reality, the penalty under the indictment as it presently exists is less than that, but it certainly includes the possibility of jail time.⁵⁹ That makes it serious enough.

I know now is not the time to do rebuttal, but I cannot help myself. There was a comment made about the Def Con-9 statements.⁶⁰ I am somewhat constrained because the case is pending and there are things that I do not want to or cannot talk about, particularly with respect to the facts of the case, and I particularly do not want to do that with government representatives on the panel and people who may be witnesses or expert witnesses in the case, so to some degree I have to circumscribe some of the things I say. But this notion about the Def Con-9 statements not being a part of the prosecution, or that is not what he is being prosecuted for, all I can say to you is that is not clear. If you go and compare the complaint and go and compare the indictment, in terms of the specific charges and there is a change

⁵⁸ See *DMCA*, *supra* note 1, § 1204.

⁵⁹ See Federal Sentencing Guidelines Manual (1998), available at <http://www.ussguide.com> (last visited Feb. 15, 2002).

⁶⁰ The Def Con-9 statements were posted on the Def Con Web site, at <http://www.defcon.org/>.

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 819

in what the government charged in the complaint and what the government charges in the indictment.⁶¹ That is, they added some aspects to the charge in the indictment.⁶² It is not at all clear that Def Con-9 and statements made at Def Con-9 are not going to play a role in the prosecution. And if they do, that may raise some additional issues, having to do with the First Amendment, which might not otherwise be present in the case.⁶³

Now, let me just give some context to the case, I think, and maybe some context to the discussion that is going to occur. First, let me tell you what the current status of the case is. It is indicted. The next appearance in the case is November 26th, and at that point in time, by agreement with the government, hopefully, we are going to have a handle on the motion practice in the case, and we expect that there is going to be, as you might expect, a whole lot of rather interesting and extensive motion practice in the case.⁶⁴ By November 26th, we are hoping to give the judge an idea of what those motions may be and some idea as to how we will do them.⁶⁵ My estimate is that this case is probably not going to go to trial until sometime next year, maybe the spring of next year, because I think the motion practice will be pretty extensive.

This is not a case about hackers or a case about piracy. That is not this case. We are talking about a legitimate company. ElcomSoft, one of my clients, is a legitimate company in Russia that for years has sold legitimate products in the United States and around the world, and in fact they sell products to federal government agencies, and in fact they sell some of their products to federal law enforcement agencies.⁶⁶ So this is not some hacker who came up with a program to sort of take the pants off of copyright owners and allow people to duplicate without regard to the rights of copyright

⁶¹ See *Sklyarov Complaint*, *supra* note 2.

⁶² *Id.*

⁶³ Robin D. Gross & Katina Bishop, *An 'Odd Bird'—A Case for Balance in Copyright Law in Cyberspace*, Electronic Frontier Foundation, at <http://www.eff.org>.

⁶⁴ See Judicial History and Documentation of *Felten v. RIAA*, No. CV-01-2660 GEB (filed June 6, 2001), Electronic Frontier Foundation, available at http://www.eff.org/IP/DMCA/Felten_v_RIAA.

⁶⁵ *Id.*

⁶⁶ See information about ElcomSoft Co. Ltd., available at <http://www.elcomsoft.com>.

owners their material. That is not what this case is about. You have to put the case in the context of a piece of software that is sold by a legitimate company. That is the context in which I think you have to ask and answer some of the questions that are raised by the prosecution in this case.

Another thing is there has been some discussion about foreign jurisdiction.⁶⁷ It does not matter. There are going to be some issues, and again, I cannot go into that, but there will be some issues about foreign jurisdiction. But for purposes of today, it does not matter. Make believe that this is a company in New York in Silicon Alley, or it is a company in California in Silicon Valley, that sells software, that is a legitimate company that sells software. That is the way we must think about it: a legitimate company selling what they believe is a legitimate product here in the United States. And, lo and behold, they find themselves being subject to—not only the company, but also an individual—criminal penalties.

There was some mention about the DMCA and what it covers. That gets to the heart of the point that I want to make today.

The DMCA really does have three, but I would say two, provisions.⁶⁸ One is a provision that concerns access control,⁶⁹ and another provision that concerns usage control, the rights of the copyright owner.⁷⁰

The access control really is intended to get to the question of authorized versus unauthorized users of the program. A case that perhaps illustrates that—and Robin can talk about that, if she wants to, a little later; she knows a lot more about this particular case than me—is the case involving DeCSS, which is the *2600.com* case.⁷¹ That is a case that really involves the issue of access control: can I actually get into and read and utilize this product, and do I have a right to read, utilize, or hear this particular product?⁷² That is access

⁶⁷ Dmitry Sklyarov wrote the program in the scope of his employment for ElcomSoft, in Russia. See *Sklyarov Complaint*, *supra* note 2.

⁶⁸ See *DMCA*, *supra* note 1, §1201.

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ See *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

⁷² See *id.*

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 821

control. That is not what this case is about. This case is not about access control.

The other part of the DMCA is the part that concerns usage control.⁷³ That is the question of protecting the exclusive rights of usage of the copyright owner.

Now, the DMCA prevents circumvention; it prevents circumvention of access controls.⁷⁴ Secondly, it prevents or it prohibits the—let’s just use the term—“manufacture of tools,” that would allow circumvention of access controls.⁷⁵ So tools are bad. You cannot circumvent access controls and you cannot make tools that would allow you to circumvent access controls.

But, you know, curiously—and maybe we will hear something about that—what it does not do is it does not prohibit circumvention of usage controls. It does not. And there is a reason for that. I think if you look at the legislative history, at least my understanding of it is that one of the reasons Congress did that is because Congress wanted to be careful not to impinge upon the fair use right or rights which were not exclusive to the copyright owner.⁷⁶ So there is no prohibition against circumvention of usage controls.

Now, the statute does, however—and I would say curiously—prohibit the manufacture of tools which could be used to circumvent usage controls.⁷⁷ That is, at least in my small-minded way of thinking, sort of a conundrum. It is interesting that if I am a user, I am allowed to circumvent usage controls, let’s say for fair use, so that I can get into this product and I can make a fair use of it, but curiously, somebody cannot make a tool that would allow me to do that.⁷⁸ I find that to be curious, and I think that is something that you are going to see talked about in the case and something that perhaps will be talked about here.

⁷³ See *DMCA*, *supra* note 1, § 1201.

⁷⁴ See *id.* § 1201(a)(1).

⁷⁵ See *id.* § 1201(a)(2).

⁷⁶ See 145 CONG. REC. S11887 (daily ed. Oct. 8, 1998), available at <http://www.hrrc.org/2281ConfReptAshcroftOct8.pdf>.

⁷⁷ See *DMCA*, *supra* note 1, § 1201(a)(2).

⁷⁸ See *Definition of Fair Use*, *supra* note 56.

It presents this circumstance: what if I have a tool that is a dual-use tool? I make a tool and it could be used in one of two ways. It could be used to do something that is illegal, that is, to circumvent an access control, but it also could be used to do something that is legal, that is, circumvention of usage controls. What is the character of that tool? Is that a tool that should be labeled “illegal,” and should I, if I manufacture it, be subject to criminal penalties? We are going to talk about that a little bit, and there is a lot to say about that.

Let me go on to another aspect of the case, employee liability.⁷⁹ You are an engineer at a software firm and what you do is you take orders from your boss and you make products and your products are sold. Now, at what point is it that you should have individual criminal liability for that product?

You know, in lots of other areas of the law—if you take the environmental area—if I stand out at the Hudson River and I take some toxic chemicals and I am an employee of the company and I stand there and I pour those chemicals into the river, well, you know what? That act of doing that subjects me to criminal liability. If I know that it is improper to do that and I stand out there and I do it for my company because they tell me to do it, I am subject to liability.

But now I am an engineer, and the company says, “I want you to make a product.” And you know what? It happens that this product is legal in ninety-nine percent of the world but it is illegal in one percent. But, by the way, I do not necessarily know that. So I make that product and the company sells it, and let’s say, hypothetically, the company sells it illegally in the one percent of the world that would prohibit it, the United States. Should that software engineer be criminally liable under those circumstances? You do not have to guess what my answer to that scenario is.

The last thing I will say is the other implication of this is something that I do have a presentation on and I talk about from time to time, and that is on the whole question of the criminalization of intellectual property law and how I think you are going to see over

⁷⁹ See *Sklyarov Complaint*, *supra* note 2. Dmitry Sklyarov was charged for developing the anti-circumvention device in the scope of his employment for ElcomSoft. *See id.*

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 823

the next five to ten years more cases like this in which issues of intellectual property are going to get resolved in criminal courts as opposed to being resolved in civil courts. I think that has tremendous implications, and maybe we will talk about that as well.

MR. BURKE: Next we have Bruce Lehman, President of the International Intellectual Property Institute.

MR. LEHMAN: Thanks.

The reason that I am here is because I was Assistant Secretary of Commerce and Commissioner of Patents and Trademarks when the original versions of the DMCA were being drafted.⁸⁰ They are the result of a White Paper that the Administration put out in 1995.⁸¹ That White Paper formed the basis of the U.S. negotiating position in Geneva when the WIPO Copyright Treaty⁸² and the WIPO Phonograms Treaty⁸³ were negotiated in 1976, and the Digital Millennium Copyright Act is the U.S. implementation of those treaties.⁸⁴ So that is the story, and I was the head of the U.S. delegation when we were negotiating those treaties.

I would like to start out by explaining the policy behind the DMCA. I have been involved in copyright law since 1974, when Congress was considering what became the 1976 Copyright Law. At the time I was counsel to the House Judiciary Committee and the subcommittee that enacted that legislation.⁸⁵

⁸⁰ Bruce Lehman was the Assistant Secretary of Commerce and Commissioner of Patents and Trademarks when the original versions of the DMCA were being drafted, from Aug. 5, 1993 to Dec. 31, 1998.

⁸¹ Information Infrastructure Task Force, Report of the Working Group on Intellectual Property Rights (1995) [hereinafter *White Paper*], available at <http://www.uspto.gov/web/offices/com/doc/ipnii/>.

⁸² See *WIPO Copyright Treaty*, *supra* note 43.

⁸³ See *WIPO Performances and Phonograms Treaty*, *supra* note 44.

⁸⁴ See *id.*; see also *WIPO Copyright Treaty*, *supra* note 43.

⁸⁵ Bruce Lehman was counsel to the House Judiciary Committee and the subcommittee that enacted the 1976 Copyright Law; see also Copyright Act of 1976, 17 U.S.C. § 101-803 (1976).

Back in 1976—and Jesse Feder has given you a flavor for what the issues were then—the issues were cable television and photocopying.⁸⁶

Back in those days, and certainly before that, if you wanted to infringe on somebody's copyright, you had to have some kind of a factory to do so. You had to have a printing press or you had to have a record plant so that you could literally make on a factory scale copies of someone's work. And so a copyright system that enabled you to sue somebody in a civil lawsuit for copyright infringement generally meant that you were going to sue someone who was in the large-scale, commercial business of copyright infringement. In the case of record piracy, it was pretty easy to track down somebody who had a record plant, to sue them and to shut them down. In the case of piracy of books, it was also pretty easy to find a printing plant and shut them down.

Now, actually photocopying was the first big problem that we had where that was not possible anymore, and a lot of 1976 was trying to catch up with that.⁸⁷ In 1976, I think people thought that since the last revision had been in 1911, we were not going to revise the copyright laws for another fifty or sixty years.⁸⁸

But technology started moving very quickly, and the Copyright Law was revised nearly every session of Congress since 1976. It is vastly different today, and almost every single one of those revisions relates to changes in technology.

A lot of them deal with this fundamental changed situation, in that infringement is no longer something that only somebody with a factory can do, that is, large-scale infringement, not an individual hand-copying a book. I am sure that people did do that from time to time in the past. I am sure people even went to the library and

⁸⁶ See H.R. REP. NO. 94-1476 (1976), 1976 WL 14045 (Leg. Hist.).

⁸⁷ *Id.*

⁸⁸ See Note, *The Criminalization of Copyright Infringement In The Digital Era*, 112 HARV. L. REV. 1705, 1706 (1999). In 1909, revisions to the Copyright Act expanded criminal penalties. These revisions provided for criminal penalties for all forms of copyright infringement except for that of sound recordings. *Id.* (citing Act of Jan. 6, 1897, ch. 4, 29 Stat. 481-82, 1707; ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT FOR THE NINETIES 548-49 (1993)).

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 825

photocopied every page of a 500-page book. But I do not know of any lawsuit that was ever brought in that situation.

Normally, this is where you would be involved, not exactly in prosecutorial discretion, but in plaintiff discretion. A plaintiff is not generally going to go out and take a case like that, because how many people are going to sit at a photocopy machine and make 500 copies of a book on a photocopy machine? They are just not going to do it, and if they want to do it, more power to them. It is a lot easier to go and just buy a copy.

And indeed, the 1976 law did recognize that there was a fair use on the part of libraries, for example, in making photocopied archival copies of books where they had gone out of print and they were not otherwise available.⁸⁹

Now, projecting forward to 1994 when I got involved in this, the issue really was copyright law for the digital age, and we were getting into the Internet age. The work that we did was a part of the Clinton Administration's National Information Infrastructure Task Force.⁹⁰ It was designed to make across-the-board policies for the Internet Age. That has actually been, I think, a remarkable effort. We have very quickly developed jurisprudence or procedures or methodologies for a whole variety of things, from privacy and security, to intellectual property right law, telecommunications policies, which have created a business environment that is secure, where people can do business in and invest in the emerging Information Society. And so that is the context of this particular work.

Now, it was very obvious that we had reached a point—and this particular case is directly the kind of fact situation that we were thinking about—we had reached a point where copyright would be virtually meaningless.

⁸⁹ 17 U.S.C. § 108 (1976).

⁹⁰ The White House formed the Information Infrastructure Task Force in 1993 to articulate and implement the Administration's vision for the National Information Infrastructure. The task force consisted of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies. See Information Infrastructure Task Force Web site [hereinafter *National Information Infrastructure Task Force*], at <http://www.iitf.nist.gov>.

Let's take the case of a e-book. If someone could buy a single authorized digital copy of an e-book and then put it up on the Internet on their Web site, just as Jesse Feder said, and then permit people to make millions of downloads, why would you go buy the book from the authorized publisher if you could do that? This is the same principle that we saw in the *Napster* case and that we are seeing in all those other copyright control cases.⁹¹

So how do we deal with that problem? We saw that problem was coming. And it seemed to us that we had gone beyond the stage at which simply the sort of basic civil law right would do the trick, that basically copyright owners were going to have to recognize that if they were going to be protected from this kind of a situation, that they would have to take some steps to protect themselves. If they did not, for all practical purposes they would just be accepting the fact that they were not going to have a lot of copyright control over their work, which people are free to do. All the time people do it, put up all kinds of valuable information on the Web and do not expect to have it controlled.

But some people do, and it is a part of their marketing strategy, and it is a part of the way their industry works, and it is in some cases the only way their industry can work to have copyright control, and so we assumed that they would want to use copy controls and that we needed to recognize that in the copyright law. So we introduced this concept of anti-circumvention legislation, that if a copyright owner used technology to try to prevent unauthorized copying, then someone who went out and deliberately created and manufactured a product that was designed to circumvent that copyright protection would be violating the copyright owner's rights.

That principle was in our White Paper and was accepted by 130 countries that were involved in the negotiation of the 1996 treaties, and is now being enacted into national laws in all of those

⁹¹ See *A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

countries.⁹² The United States just happened to be the first, and the Digital Millennium Copyright Act was the expression of that treaty.⁹³

Now, I would like to make a comment about fair use because this is really an issue that I feel is so misrepresented oftentimes, what fair use is and what it is not. Fair use really is the intersection between the First Amendment and the Copyright Law, both of which are grounded in the Constitution.⁹⁴ Historically, fair use in this country was the right of quotation.⁹⁵ It was not really until the photocopying cases—and we really only had one Supreme Court case on that, which was a split decision, *Wilkins v. Williams*, it was not really until the photocopying era that fair use was anything other than the right of quotation.⁹⁶

To get back to a point that Jesse Feder made before, as I see fair use, fair use is your right to take somebody else's work and to copy parts of it—not all of it, but parts of it—for the purpose of comment, criticism, satire, et cetera. That is a part of your First Amendment right. Fair use never contemplated the right to make thousands or millions of complete, perfect copies of someone else's work or to enable that process.⁹⁷

The implications of that, if fair use is to be extended to that level of being able to make thousands of copies in an authorized way, means that the copyright law in the modern technological era simply becomes meaningless, and all of the industries that are based on it. What is going to happen to the publishing industry in New York when everyone gets books electronically, maybe not next year but maybe twenty years from now, what is going to happen to it if there is simply no capacity for this kind of copy control? It will not exist.

That is why this was a part of the Clinton Administration's overall National Information Infrastructure Policy Review, it is because we needed to create rules and regulations for the information industries

⁹² See *White Paper*, *supra* note 81; see also *WIPO Copyright Treaty*, *supra* note 43.

⁹³ See *DMCA*, *supra* note 1.

⁹⁴ U.S. CONST. art. I, § 8, cl. 8; U.S. CONST. amend. I; Copyright Act of 1976, 17 U.S.C. §§ 101-803; *DMCA*, *supra* note 1.

⁹⁵ See *Definition of Fair Use*, *supra* note 56.

⁹⁶ *Wilkins v. Williams*, 580 F.2d 1050 (4th Cir. 1978), *cert denied*, 439 U.S. 1118 (1979).

⁹⁷ See *Definition of Fair Use*, *supra* note 56.

which are going to be at the very heart of economic growth in the United States in the coming decades.⁹⁸ We need to create a foundation for those industries to be secure and to grow, and for people to make judgments about how they wanted to use the law.

We have always had publications that have been made available for free; that will continue to be the case. Where someone chooses to restrict the distribution of their work, the law needs to provide for that, it needs to provide effective protections, and that was the origin of the DMCA.⁹⁹

MR. BURKE: Thank you.

Next we have Robin Gross, who is an intellectual property attorney and director of the Electronic Frontier Foundation's (hereinafter "EFF") Campaign for Audio-Visual Free Expression. Robin?

MS. GROSS: The EFF's concern with the DMCA is really that it tips the balance too far in favor of the copyright industry at the expense of the public's rights. Although Copyright Law intentionally places limits on copyright holders' rights to control uses of their work, the DMCA gives complete control to copyright holders to control all uses of a copyrighted work, and this tramples on fair use, it tramples on public domain rights, and other rights of the individuals.

The Supreme Court has held that fair use is the breathing space that is required by the First Amendment in copyright law.¹⁰⁰ But the DMCA has effectively eliminated fair use.

The tool that Dmitry Sklyarov wrote is necessary for the public to exercise its fair use rights. So the idea that this is not a case about fair use is really misguided, because it is the public's fair use rights that are implicated here. They need this tool in order to exercise their rights.

⁹⁸ See *National Information Infrastructure Task Force*, *supra* note 90.

⁹⁹ See *DMCA*, *supra* note 1.

¹⁰⁰ See *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539 (1985).

The tool that Dmitry wrote is necessary for people to read their e-book that they downloaded at work onto their laptop at home; blind folks need this program in order to be able to have the text of their books read to them; if you need to be able to copy a page for a school report—all of these things are lawful uses that this program enables. No one is debating that these are lawful uses and that the program enables these uses.

It is really important to realize that the only people for whom this tool is at all useful is someone who has legally paid for and downloaded an Adobe Ebook. This is not a case about piracy. This is just a case where people have purchased an e-book and simply want to be able to view it in other ways.

Claims that fair use only applies to the right of quotations or copying in small part ignore solid case law on this issue. The Supreme Court held, in the *Betamax* case, that copying entire movies and entire television programs for purposes of time-shifting is a fair use that the public has a right to engage in.¹⁰¹ The *Diamond/RIAA* court a couple of years ago held that the public has a fair use right to make entire copies of their music collection on their computers.¹⁰² So be very careful when you hear these claims about what fair use is and is not, and I suggest you read the case law.

History has taught us that every time a new technology comes out—whether it is piano rolls, or VCRs—the copyright industry has reacted by claiming that because this technology is new and better than what we have had in the past, it poses too great of a danger to the ability to profit to be allowed in the hands of the public. Yet, in each one of these cases the courts have prevented the industry from outlawing the technology and the industry has found a way to profit from the new opportunities that the technology brings about.¹⁰³

¹⁰¹ See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

¹⁰² See *Recording Indus. Ass'n of Am. v. Diamond Multimedia Systems, Inc.*, 180 F.3d 1072 (9th Cir. 1999).

¹⁰³ See *White-Smith Music Publishing Co. v. Apollo Co.*, 209 U.S. 1 (1908) (piano rolls); *Sony*, 464 U.S. at 417 (1984) (video cassette recorders).

There is some talk about exemptions in the DMCA that help to enable lawful uses.¹⁰⁴ These exemptions are completely useless. The exemptions in the statute's ban on circumvention are so narrow and apply to such a small number of situations in which people would actually need to circumvent that they have not been able to be relied on by a single person yet who has tried to rely on them in the courts.

For example, the encryption exemption does not cover access tools, only copy tools, so that does not help most researchers because these two functions are often combined together in the same technology, so you cannot do the one without doing the other, which you are forbidden from doing.¹⁰⁵

Also, the exemption on reverse-engineering only applies to computer programs and solely for the purposes of interoperability.¹⁰⁶ This is too limiting to incorporate most reverse-engineering needs.

So the DMCA leaves the public with weak security, hobbled technology, and muzzled professors. Bank records, telephones, electricity, medical records, e-mail communications, all depend upon the highest level of security to ensure people are to protect themselves in the electronic world, but the DMCA weakens the public security because scientists can no longer test the security of a system and learn if it is vulnerable to attack. So the DMCA is actually used to prevent the public from obtaining the truth about the vulnerabilities of the security systems that they are using.

Now, the DMCA may be law in the United States, but it is stifling science and chilling speech all over the world. Since Dmitry's arrest, and Professor Felten, a Princeton University computer scientist, was threatened with litigation under the DMCA when he wanted to publish his research,¹⁰⁷ and the *2600.com* case where a journalist was

¹⁰⁴ See generally Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, available at <http://www.loc.gov/copyright/1201/anticirc.html> (last visited Feb. 2, 2002).

¹⁰⁵ See *DMCA*, supra note 1, § 1201(g).

¹⁰⁶ See *DMCA*, supra note 1, § 1201(f).

¹⁰⁷ See Cindy Cohn & Robin Gross, *EFF Protects Scientists' Speech in RIAA Case: Government, Record Industry Disagree on Digital Copyright Law*, The Electronic Frontier Foundation, October 25, 2001, available at <http://www.eff.org>; see also *Felten v. Recording*

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 831

forced to remove information from his Web site under the DMCA,¹⁰⁸ several prominent foreign scientists have issued statements expressing their fear to travel to the United States since this statute has been enacted. So scientists all over the world now have to ask themselves if some research they have done or a computer program that they have written could likewise subject them to DMCA liability if they were to travel to this country.

Technical and scientific conferences are moving overseas, since the conference organizers risk liability for themselves and their speakers if they go forward in the United States.¹⁰⁹ And because these conferences are done for profit, the criminal provisions are triggered. So that is why we have conferences moving overseas.

In fact, Russia has even issued a travel advisory warning computer programmers about the dangers that they face since the DMCA was passed if they want to travel to this country.¹¹⁰

Well, the sky may not be falling, but we are chilling science, innovation, and speech. And this idea about jailing programmers for writing software with legitimate uses, this is really a new concept. Holding employees liable for the acts of their companies is quite astonishing. I mean, do we do this for guns? Do we hold the folks who work in the factories and make the guns liable for the killings that occur with those guns? We do not. Yet we are trying to do that for copyright here.

Well, some claim that the DMCA was enacted to implement the United States' treaty obligations under WIPO. However, during the congressional hearings on the DMCA, Administration officials admitted during testimony that the anti-circumvention provisions in Section 1201 were not required by the treaties, that they went farther

Indus. Ass'n of Am., No. CV-01-2660 (D.N.J. filed 2001), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

¹⁰⁸ See *Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

¹⁰⁹ See generally Electronic Frontier Foundation documents related to *Felten v. RIAA*, available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/felten_legal_documents.html.

¹¹⁰ See generally Electronic Frontier Foundation materials related to *United States v. Sklyarov*, available at http://www.eff.org/IP/DMCA/US_v_Sklyarov/us_v_sklyarov_faq.html.

than the treaties required.¹¹¹ The treaties only required signatory countries to provide adequate legal protection and effective legal remedies.¹¹²

The U.S. Copyright Law already contained adequate legal protection and remedies to meet the U.S. treaty requirements without enacting the DMCA. These would be found in the theories of contributory and vicarious liability, which were the theories that Napster was just found likely to have violated.¹¹³

So our obligations under the WIPO treaties really only required us to enact a ban against illegal acts. However, the DMCA went farther and banned tools, and it did not have to do this.

Congress intended the DMCA to apply to black boxes, not devices with substantial non-infringing uses, or to jail software programmers. Congress thought it was passing a bill to aid in the prevention of infringement. But the DMCA, as enforced, is far broader than that and applies to people engaging in substantial amounts of lawful speech. In fact, the current U.S. Attorney General, John Ashcroft, is quoted all throughout the legislative history when he was a senator as stating that the DMCA did not apply to devices with substantial non-infringing uses and that the *Betamax* doctrine remained the rule.¹¹⁴ The *Betamax* doctrine states that devices with substantial non-infringing uses cannot be outlawed.¹¹⁵

One thing that we hear an awful lot about is all the dangers that digital technology provides to copyright holders. But it is really important to realize that digital technology changes things on both sides of the equation, and copyright imposes rights, as well as responsibilities, on authors and on the public. So it is really not fair

¹¹¹ See 145 CONG. REC. S11890 (daily ed. Oct. 8, 1998), available at www.hrrc.org/2281ConfReptLeahyOct8.pdf.

¹¹² See *WIPO Copyright Treaty*, *supra* note 43; see also *WIPO Performances and Phonograms Treaty*, *supra* note 44.

¹¹³ See *Napster*, 114 F. Supp. 2d at 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

¹¹⁴ See 145 CONG. REC. S11887 (daily ed. Oct. 8, 1998), available at <http://www.hrrc.org/2281ConfReptAshcroftOct8.pdf>; see also *Sony*, 464 U.S. at 417 (1984).

¹¹⁵ See *Sony*, 464 U.S. at 417 (1984).

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 833

for one side to take all of the benefit and accept none of the responsibility in the copyright bargain, and this applies both to authors and to the public. The public must ensure that the artists are economically rewarded for their creative gifts. Likewise, the authors must ensure that the public is able to retain its rights and abilities to use and access creative expression.

In its zeal to stamp out infringement, industry has used the DMCA to silence a substantial amount of lawful speech; it has been used to squelch the research of a Princeton professor about the weaknesses in the recording industry's controls for digital music,¹¹⁶ gag a journalist who has published information about the movie studios' encryption scheme through DVDs,¹¹⁷ smash a competitor ElcomSoft for creating software that can inter-operate with Adobe's Ebooks.¹¹⁸ Yet, in none of these cases has anyone been accused of any copyright infringement.

The DMCA is clearly chilling speech and research here, it is being used to create a monopoly on building devices that can read a file, and this is essentially establishing a leak-proof pipe for information distribution. Hollywood asked Congress for the DMCA back in 1998 to be used as a shield against infringement. Now that it is law, Hollywood uses the DMCA as a sword to prevent competition, take away fair use rights, and control information distribution, as well as censoring data about technologies' vulnerabilities.

In summary, I would just like to say that the DMCA, as enforced, is chilling speech, science, innovation, ignoring the public's fair use rights, ignoring the public domain. Until we can get some kind of balance put back into copyright law that recognizes that the public has rights here and that the copyright holders have responsibilities, this problem is only going to get worse.

Thank you.

¹¹⁶ See *Felten v. Recording Indus. Ass'n of Am.*, No. CV-01-2660 (D.N.J. filed 2001), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

¹¹⁷ See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

¹¹⁸ See *Sklyarov Complaint*, *supra* note 2.

MR. BURKE: Now we have Eric Smith, who is a Partner at Smith & Metalitz.

MR. SMITH: Thank you very much.

Robin, you have, I think, left us all breathless with your presentation. I will try to respond to some of your points, but I am not going to get to all of them.

Robin essentially has created a “right of circumvention.” The difficulty with her position, I think, is that Congress considered carefully, in the legislation and in the House and Senate Reports, virtually every assertion that was just made and disagreed with them.¹¹⁹ Congress, in fact, intended specifically to get at, for example, access controls that do not involve infringement, Congress did not intend just to deal with technological measures that protected against infringement. It went right to access, and it says so right (a) in the legislation and (b) in the Reports. I would encourage all of you to pick up those reports and read them very carefully.

The difficulty for the opponents of § 1201 is that Congress was aware of all of these issues—fair use issues, the fact that the encryption technology could lock up public domain works, could in certain cases prevent the exercise of fair use rights, and made a very difficult balancing decision that opted for Section 1201 with carefully crafted exceptions which, frankly, I do not think are useless at all—at least, the people who lobbied them did not think that they were useless.¹²⁰

Let me just respond to a couple of other points. I do not have a lot of time.

First, it was mentioned that the act of circumvention, however defined—copy control, access control—and, by the way, the Justice Department could have charged an (a)(2) violation, an access control violation, because in fact once the key is stripped out—and this is in

¹¹⁹ See generally H.R. CONF. REP. NO. 105-796 (1998); H.R. 2281, 105th Cong. (2d Sess. 1998) (legislative history of the DMCA) [hereinafter *H.R. Conf. Rep.*]; S. REP. NO. 105-190 (1998); H.R. REP. NO. 105-551 (1998).

¹²⁰ 17 U.S.C.A. § 1201 (c)-(g) (West Supp. 1999); see also *H.R. Conf. Rep.*; S. REP. NO. 105-190 (1998); H.R. REP. NO. 105-551 (1998).

the clear—everyone has access to this work without the permission of the copyright owner.¹²¹ So there is an interrelationship. Access controls and copy controls very often overlap.

One assertion was that “it is legal in the rest of the world.” Well, that is just not true. Circumventing technological protection measures is illegal in Ireland, it is illegal in Japan, it is illegal in Australia, though Australia has some exceptions that we do not have in our law.¹²² It will soon be illegal even in Russia. Now, if I say, “exactly this conduct,” I am not suggesting that in the case of Mr. Sklyarov that the Justice Department is going to prove all that they have in the indictment, but I am saying that, based on what is in the indictment, it would be illegal under the Russian draft law. Reason: They signed the Treaty in 1996 and they are going to become a member of the Treaty, they are going to do all of this, including anti-circumvention controls.¹²³

Another assertion: “this law gives copyright owners what they did not have before.” Well, I do not agree with that. We have had technological protection against signal theft for many, many years with respect to audio-visual works.¹²⁴ You cannot sell a black box that will defeat encryption on a pay satellite signal.¹²⁵ Now, while that is not the Internet—it is a different, older technology—but it is the same thing with just an analog technology, and nobody claimed fair use or First Amendment rights when that bill was passed. Maybe they did, I was not involved at that time—but remember that these objections to § 1201 deal with the Internet, they are based on

¹²¹ See 17 U.S.C. § 1201(a)(2).

¹²² Copyright and Related Rights Act, Part VII, Ch. 1 § 370 (Ireland Jan. 1, 2001); Copyright Act of Japan, Law No. 48, 1970, art. 120-2; Copyright Act of 1968, Pt. V, Div. 2A, Section 116A (Austl.).

¹²³ See *WIPO Copyright Treaty*, *supra* note 43; see also *WIPO Performances and Phonograms Treaty*, *supra* note 44.

¹²⁴ See 47 U.S.C. § 605(4) enacted in 1984 which reads as follows:

Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a), shall be fined not more than \$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both.

¹²⁵ See, e.g., *Premier Communications Network, Inc. v. Fuentes*, 880 F.2d 1096 (9th Cir. 1989).

the ideology of the Internet, not necessarily with the issue of access and copy controls, because we have had them under U.S. law before, and other countries have them as well.¹²⁶

On the First Amendment: I would hope that the Justice Department does not prosecute Mr. Sklyarov for what he “said” at Def Con. That would be terrible. That would be a violation of his First Amendment rights. The indictment does not suggest that he is being prosecuted for that.

Now, in the *Napster* case, for example, what the owner of Napster said in First Amendment-protected advertising and other speech was evidence of what the primary purpose and intent of the Napster service was, as Judge Patel said, so you can use his speech there—I am not sure the Justice Department will use it, but they could use it, as evidence of certain aspects of the indictment.¹²⁷

Mr. Burton mentioned that Elcomsoft is “a legitimate company.” Yes, it is a legitimate company. It provided password recovery software. My business is as President of the International Intellectual Property Alliance, which represents, for those of you who do not know, 1,100 companies that cut across all the copyright industries.¹²⁸ Our target is global piracy. There are many, many CD factories, for example in Asia, that are “legitimate companies” where employees of those companies are now sitting in jail in those countries because as legal companies they operated at night illegally manufacturing pirate CDs and exporting them on a global basis. So yes, it is a legal company, but it went wrong here. And I think they knew they went wrong. I think the evidence will establish, based on

¹²⁶ See, e.g., the North American Free Trade Agreement (1993) between the U.S., Canada and Mexico which in Part Six, Chapter 17, Article 1707, obligates the signatories to provide protection for encrypted program-carrying satellite signals including making it a criminal offense “to manufacture, import, sell, lease, or otherwise make available a device or system that is primarily of assistance in decoding an encrypted program-carrying satellite signal without the authorization of the lawful distributor of that signal.”; see also Art. 145 “Ley Federal del Derecho de Autor,” [Copyright Act of Mexico] D.O., 24 de diciembre de 1996, (amended March 27, 1997).

¹²⁷ See *Napster*, 114 F. Supp. 2d 896, at 922-923 (N.D. Cal. 2000), *aff’d in part, rev’d in part*, 239 F.3d 1004 (9th Cir. 2001).

¹²⁸ The International Intellectual Property Alliance Web site may be accessed at <http://www.iipa.com>.

the press reports, that ElcomSoft and Mr. Sklyarov knew exactly what they were doing when they came to the United States to sell this software.

Mr. Burton mentioned “IP issues in criminal courts.” Copyright infringement has been a criminal violation for as long as I know, and it is a criminal violation in every country in the world that has a copyright law.¹²⁹ I disagree that Congress felt that “adequate legal protection and effective legal remedies,” under Article 13 of the WCT and the corresponding articles of the WPPT, were already covered by the Copyright Law.¹³⁰ Congress specifically said that these protections were not covered by the Copyright Law. It is right in the reports. It is right in the legislation. Congress established separate criminal penalties, without regard to infringement, for circumvention technologies that defeated access controls.¹³¹

It was asserted that “the exemptions in § 1201 are useless.” The point was made, I think, that encryption researchers cannot do their business. In fact, if you look at the statute and look at the reports, encryption researchers are permitted to use circumvention tools; they just cannot put them on the open market for a price. It is right in the statute. And they can even take those encryption tools and use them, collaborate with other people to use them, so long as they act in good faith and they meet the criteria in the statute, one of which is not facilitating infringement.¹³²

So ElcomSoft did inform the copyright owner of the weaknesses in the Adobe encryption, but if you are an encryption researcher, you do not have to sell the program that you are doing research on or the program that allows you to decrypt something. That is a commercial venture, not research.

Finally, I wanted to say something more about the First Amendment. I think Judge Kaplan, in the *Reimerdes* case (the so-

¹²⁹ See Copyright Act of 1976, 17 U.S.C. § 506 and 18 U.S.C. § 2319.

¹³⁰ See *WIPO Copyright Treaty*, *supra* note 43; see also *WIPO Performances and Phonograms Treaty*, *supra* note 44; S. REP. NO. 105-190, at 11 (1998).

¹³¹ 17 U.S.C. § 1204 (1998).

¹³² 17 U.S.C. § 1201(g) (1998).

called *DeCSS* case),¹³³ covered pretty well the First Amendment issues that are involved in that case, which is not dissimilar to this case. That case involved a piece of software that decrypted the DVD encryption technology. Involved here is a piece of software that decrypts the Adobe encryption system.

I think Judge Kaplan in that case went through the First Amendment analysis, which, by the way, I agree can undermine or defeat this statutory scheme—indeed, it is the only thing that can undermine it—because fair use and all the other issues that were talked about here are not of a constitutional dimension. These other issues are for Congress to decide what the policy is, and Congress decided what the policy was. Some of us may disagree with that policy determination, but it is what Congress said. And obviously, if that scheme violates the First Amendment, the courts are going to strike that part down. I do not think it violates the First Amendment.

Yes, software has expressive elements, but Judge Kaplan said, in no uncertain terms, that here in this situation, while software is protected by the First Amendment, the level of protection was much lower because it was the functionality of the software that was the real issue there; that because there was a strong governmental interest and there was a lower level of protection, the First Amendment was not violated.¹³⁴ Now, the case is on appeal to the Second Circuit.¹³⁵ Because the *DeCSS* case was a linking case, there may be some interesting First Amendment issues that deal specifically with linking, which are not present in the *Sklyarov* case.

I have talked too long, but I hope these remarks will spark your thinking, and we all look forward to continuing this dialogue.

Thank you.

¹³³ *Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

¹³⁴ *See id.* at 332-33.

¹³⁵ Since the date of this presentation, the Second Circuit has ruled, upholding Judge Kaplan's First Amendment discussion regarding posting of *DeCSS* and linking to *DeCSS*. *See Universal Studios, Inc. v. Corley*, 273 F.3d 429, 453-58 (2001).

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 839

MR. BURKE: Finally, we have Mark Cohen, who is here from the Patent and Trademark Office, who is going to give some commentary on what he has heard.

MR. COHEN: In hearing this discussion, I am reminded a little bit of an anecdote that a professor at Stanford Law School once told me about a trip he made in China in the late 1970s and early 1980s. He was sitting next to a Chinese manager when there was an announcement on the loudspeaker that China had enacted a new contract law. The manager said, "We will never use that." And, of course, things have changed.

I think Eric Smith's comment that the Russian Duma enacted protection for TPMs on September 12th, if I heard him correctly?

MR. SMITH: They did not enact it. They introduced the legislation.

MR. COHEN: They introduced it. That is perhaps one indication of that.

We have heard a lot about the Digital Age, and I think Mr. Burton has also talked about the business environment, and others in the history of the DMCA, is how some of these things might play out in the countries where people like Mr. Sklyarov came from. I think it is important to keep in mind that those business environments are rather different from our own, and the history of protection of property rights is rather short-lived.

The Chinese example again is 1983 was the first patent law in China, and traditionally there were not patents.¹³⁶ There were inventor certificates, and the rights given to individuals were very limited.¹³⁷

And especially, interestingly enough, in trade secrets, which is perhaps somewhat analogous to this, trade secret protection is often minimal. Internationally, trade secret protection is important because

¹³⁶ See generally Ramona L. Taylor, *Tearing Down the Great Wall: China's Road to WTO Accession*, 41 J.L. & TECH. 151 (2001) (citing 1983 Patent Law of China).

¹³⁷ *Id.*

it is an unknown right, how to protect your interests in the information you create.

So this is something that is an emerging issue for these countries, but that does not mean that protection of it is any less valid, nor does it mean that protection in the international sphere is less valid. I think, again, Mr. Burton's comments about what does the future carry for criminalization of IP rights is a question for a futurist, which I am not, but there are obviously more and more cases of this type.

And again to make the analogy to trade secret protection, there is a case now in the District of New Jersey involving theft of trade secrets by Chinese employees of Lucent,¹³⁸ which again people may not understand the rights that we accord in this country to IP rights, and I guess they just have to learn it, and they will learn it when they recognize that the laws will equally develop their own systems as they protect their own.

The idea, which I also found interesting, that Russia now issues a travel advisory, that is not so uncommon. Obviously, if people get caught up in the criminal system, they want to protect their citizens.

Another point, which I think is also directed perhaps to culture clashes, is employees of companies. We have heard whether it is correct or justified to prosecute an employee of a legitimate company. Now, whether they are in fact legitimate or not, or one hundred percent legitimate, I think Eric addressed that issue.

It is unfortunate that many countries throughout the world do not provide whistle-blowing protection, so that employees that are in those positions may find that their livelihood will be compromised, and perhaps IP laws will be one vehicle towards encouraging employees acting in accordance with the law once Russia enacts a law of that nature.

Those are my general comments.

¹³⁸ See Simon Romero, *F.B.I. Says 3 Stole Secrets From Lucent*, N.Y. TIMES, May 4, 2001, at C1.

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 841

MR. BURKE: Maybe we should just turn it over to the audience so that we can hear your questions. But first, I have one question for the panel.

One thing that confuses me in this debate—the issue of fair use. I think the concept is really misunderstood by a lot of people. As I understand this case, if you use the Adobe product, the eBook Reader that they have, the only thing you can do as the purchaser of that e-book is to play it and view it on the machine where you actually receive it, and that the publisher—maybe not Adobe, but the publisher—has a right to restrict any further actions on your part, whether that is to copy a portion of the book. Let's say it is a professor who wants to take a paragraph, which typically under fair use would be acceptable and legal, or to make those kinds of limited uses of the book.

Is that correct here?

MR. SMITH: I think Congress made a judgment that the danger from unauthorized copying and further distribution of digitally transmitted material was so high, that there could be some incursions on fair use.

MR. BURKE: So my question is: does this wipe it out totally?

MR. SMITH: No, I do not think it wipes it out. For one thing, obviously this material will normally be available in a format that is not encrypted. You know, a lot of these e-books will be published as normal, printed books. I think they are published as e-books because they are much, much cheaper than the hard copy, and that is why digitization is such a good thing for the public.

But I think Congress was aware of this problem, and one of the reasons that they included a provision for a three-year study, which was just completed, that Jesse's office just did, was to look and make sure that the damage to fair use was not inappropriate, had not gone too far.¹³⁹

And frankly, technology is going to advance as we move forward, I think, and it will become much more granular, such that, for

¹³⁹ See *White Paper*, *supra* note 81.

example, a public domain work that is put inside a database with protected works may in fact be watermarked so that you could get access to it. We cannot do that now with the present technology, but as we move further down the road, some of these issues may go away, in a sense, or the worst part of some of these issues, or what we think are the worst parts of some of these issues, may go away as technology advances.

But right now we do not have the technology, and Congress said: “Yes, there will be some incursions here, but on balance, after thinking about it very carefully, this is our decision.”

MR. LEHMAN: This is not about any restrictions that Adobe may have put on the use of the book. Those would be license restrictions, like a shrink-wrap license when you buy any piece of software.¹⁴⁰ This is about marketing a device that enables you to defeat the encryption.

Now, if people do not like Adobe’s licensing provisions, then they can choose not to buy Adobe’s books. In fact, we found in the early days of the computer software industry in this country, when people tried to use copy protection, there was a lot of market resistance and a lot of companies stopped using it.

So you have to distinguish between the licensing provisions that a company might put in and this provision of the Copyright Law.

And furthermore, what we are talking about here, even if you do want to take a paragraph from it, is the ability to directly download from that program snippets of the work. Apparently, this probably does not permit you to do that. But absolutely nothing under the law stops you from displaying the text on the screen and sitting there and typing into your own hard drive whatever portions of the book you want to type in.

MR. BURTON: I am sorry. I do not mean to interrupt, but I thought I heard you say that nothing would stop the individual from, after removing, as you call it, the Adobe encryption, nothing would

¹⁴⁰ See *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). Shrink-wrap licenses are terms shipped along with software to purchasers intending to form a contract with the seller. See *id.*

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 843

stop that individual from using it there on their laptop or a home computer?

MR. LEHMAN: No, that is not what I said. Nothing would stop you when you display the work on the screen, presumably of your computer or your appliance, nothing stops you from then copying what you see on the display in a separate fixation device, whether it is a pen and paper or whether it is your computer.

MR. BURTON: How about another computer that is yours?

MR. LEHMAN: In other words, all that is prevented by the encryption is your downloading the work electronically. It does not stop you from making some other form. It does not stop you from copying the old-fashioned way.

MR. BURTON: Copying it from where to where? I honestly do not understand. Copy it from where to where?

MR. SMITH: The old-fashioned way.

MR. LEHMAN: Taking your pen and writing it down. We do not use typewriters much any more, but every computer has your own Microsoft Word or WordPerfect on it, and you are entitled to sit there and type to your heart's content.

MR. BURKE: But let's say that we have a picture. Let's say there is a picture in a book that you as a professor want to use in a lecture that typically you would be able to do, you would be able to copy it.

MR. LEHMAN: Scan it. I think you could probably scan it.

MS. GROSS: Not if the scanner would not let you because it recognized the technology.

MR. LEHMAN: Well, if it would not, then this gets to this market question. I mean, when you buy the product, you know that that is what you are getting. Then go down and buy the paper version of the book.

MR. FEDER: Again, you could also photograph it. The point is that the ability to make a perfect digital reproduction of something is

not something that is inherent in fair use. Fair use entails copying, but it does not have to be a perfect digital reproduction.

MR. BURKE: So it is more cumbersome. You are saying that the right is potentially more cumbersome than it was before, but it still exists in some form?

MR. LEHMAN: It is not more cumbersome at all. It is just exactly the same as it has always been.

MR. BURKE: Well, if you have to go and get a camera and take a photograph of an image on your computer, as opposed to taking a book and bringing it to the Xerox machine, it seems to me that it is more difficult.

MR. LEHMAN: Well, you know, fifty years ago we did not have Xerox machines and the only way that you could exercise fair use in a photograph would be to do that, although let me say that making willy-nilly photographs of an entire work in itself, unless it is for a very restricted purpose, does violate fair use. The notion that somehow or other we can go photograph and then distribute many, many copies of a photograph or other pictorial graphic work is definitely not encompassed by fair use.

MR. BURKE: And just because you can do something does not mean you have the right to do something. If it violates the Constitution, you would have a right vis-à-vis what Congress has decided is the balance in this area. Congress has made this decision. It may not be the right one. We may decide we do not like it after awhile. I do not think so, but if it is not a constitutional violation, then it is Congress's decision how to balance these rights.

MS. GROSS: I actually take issue with that. Congress creates a balance and many do not like the balance here. The balance that we are seeing is total control to the copyright industry. What kind of balance is that? And I do not think that is the kind of balance that Congress thought it was creating.

And this idea that the DMCA is nothing new because we have had laws against cable and satellite black boxes is also misleading. Those laws apply to intercepting something that you have not paid

for, that you do not have a right to. But the DMCA is being used to prevent you from accessing and using things that you own, that you purchased, that you are trying to use in the privacy of your own home in the way that works for you. This is not about piracy. This is about control.

MR. LEHMAN: Well, that is the first sale doctrine really that you are talking about there, and what rights you might have under that.¹⁴¹

MR. SMITH: One of the things that has been interesting is that this software somehow is limited to taking the encryption off only a legal copy. Who says? If somebody decides—I know this is kind of unusual—but if somebody takes an encrypted version of an e-book and does not have any rights to sell it on the Internet and puts it up encrypted and charges fifty dollars for it, as pirates will—believe me they will, just like ElcomSoft put encryption around their program when they sold it for \$99—what is to prevent a pirate from selling an encrypted version, and this ElcomSoft software will decrypt it and allow everybody to use it?

MR. BURTON: Well, then what you do is you make a law that goes after the pirate. You do not make a law that goes after the person who made the tool, which can be used either by pirates or could be used by an individual for legitimate uses. That is how you handle the situation of somebody who is going to take it and distribute it. ElcomSoft did not do that. ElcomSoft *did not do that*. ElcomSoft made a tool.

Now, if somebody wanted to use that tool to distribute 5,000 copies of the book, or 5 million, then you prosecute the people who

¹⁴¹ See JOYCE ET AL., *supra* note 56. Traditionally, copyright owners have had the right to retain their works confidentially (never license the work), but once the first license was issued, the owner was prohibited from barring or demanding a royalty from subsequent published works. The first sale doctrine is a defense to a claim of infringement of a copyright holder's right to publicly distribute copies of the work. Thus, it acts as a limitation on the scope of the public distribution right. The first sale doctrine is codified at 17 U.S.C. § 109(a). *Id.*; see, e.g., David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 710-11 (2000). Under the DMCA the first sale doctrine is undermined because it does not take effect if a creator encrypts all copies, even subsequently made "legal" copies, of his or her work with anti-circumvention devices. *See id.*

did that, not the person who made the tool so that I can have a fair use of that book, which means perhaps putting it from my desktop machine to my laptop. That is how you handle it.

MR. LEHMAN: The problem here is that the person who is actually making the unauthorized copy when something is sent out on the Internet en masse is actually the end-user. I think one of the things about the Copyright Law is it can never work successfully if you are going to go after each individual end-user. That is why, as I said in my earlier remarks, historically you went after the choke points, you went after the people who had the factory that produced the illegal copies.

That was exactly the theory here behind the work that we did in the DMCA, is that it is precisely people like ElcomSoft who are just like that factory that would have produced the illegal records. They are the commercial entity that is abetting wide-scale piracy.

MR. BURTON: Well, but what you do in that circumstance then is what is done in most criminal laws, is you tie the intent of the tool maker to the illegal activity. You do not just outlaw in a blanket fashion the activity of making the tool.

And by the way, this notion that the satellite system—I defy anybody to find me a federal criminal statute like this. Every other federal statute ties the intent of the maker of the tool to the illegal activity and it is on the face of the statute. There is no other statute that I have ever seen, and I have been doing this for thirty years, that is like this.

MR. SMITH: Well, I guess maybe I would put it a different way. If I make a black box to steal a satellite signal or I write the software and put it on the chip and then sell the chip to put in the black box, and I am a software programmer, I am criminally liable if I sell that software.

MR. BURTON: If you have the intent that it be used in an illegal way.

MR. SMITH: Well, Congress said it was illegal to make a device that circumvented a technological protection measure, and

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 847

ElcomSoft and Mr. Sklyarov had such an intent. They may have been ignorant of our law, but they had an intent to do what they did, which violates the law.

MR. LEHMAN: Well, there are all kinds of criminal statutes that do not require intent, period.

MR. BURTON: Of course. That is not what I said.

MR. LEHMAN: You know, intent is not a basic requirement of criminal law.

MR. BURTON: Well, it is in this case, though.

MR. LEHMAN: It can be an element of the degree. It can be an element of whether something was willful, but you can absolutely unknowingly violate criminal laws, and people do it all the time.

MR. BURKE: Let me just jump to the floor here. We have a question up there.

QUESTIONER: My name is David Perry-Campf. I am a second-year student here and a staff member of the *Fordham IPLJ*.

I have a question, and that is: We are talking about fair use. Is not the problem that, instead of Judge Patel in the *Napster* case¹⁴² getting to decide whether Napster represents a substantial fair use under the *Betamax* standard,¹⁴³ now we have corporations deciding what is fair use and then writing software that protects what that fair use is, and in any attempt to circumvent that technology the person is then faced with prosecution under the DMCA? In other words, we are not protecting copyright users. Mr. Smith, you said this. We are not trying to protect copyright users. We are merely blocking access and we are protecting companies that block access.

My question is: Who is the DMCA trying to protect? Seventy-four million people knowingly violated copyright law in *Napster*.¹⁴⁴ Is

¹⁴² See *Napster*, 114 F. Supp. 2d at 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

¹⁴³ See *Sony*, 464 U.S. at 417 (1984).

¹⁴⁴ See *Napster*, 114 F. Supp. 2d at 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

that not a kind of civil disobedience illuminating what people actually care about in terms of copyright law?

MR. LEHMAN: It was civil disobedience, and I was in the Clinton Administration, and we decided, “damn it, we are not going to let it happen,” and that is what the DMCA is all about, and it is the law of the land, and you will see it put into effect in this case. You may not like it, but you have a Congress that considered all of these things. Many of you in this room probably intend on making your living in the publishing- and the entertainment-based industry. If you want to have a job, you are not going to have many jobs defending guys like Mr. Sklyarov.

QUESTIONER: This question is for Mr. Burton. Mr. Burton, I think your tool metaphor is a good metaphor, but I want to know how you address the fact that your client was speaking at Def Con, and perhaps you could share for some people what Def Con actually is all about.

MR. BURTON: Well, let me take it back. Def Con is the largest of the security industry conventions.¹⁴⁵ Now, it started out as a convention that was attended and started by hackers, whatever that means, and hackers did not necessarily mean individuals who were involved in illegal activity. But it started in the sort of hacker community, and there is a lot of fight over what hacker means, but that is where it started.

But it certainly has progressed over the last several years to be the premier security industry. The FBI is there, lots of organizations are there, and they are not hiding, they are out in the open.

MR. GROSS: Would you define hacking?

MR. BURTON: And they are also there giving presentations about computer programs and computer security.

MR. GROSS: Joe, could you define hacking? What is your definition?

¹⁴⁵ See Def Con Web site, Information on Def Con, at <http://www.defcon.org> (identifying Def Con as “the largest underground security gathering on the planet”).

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 849

MR. BURTON: Let Robin define it.

MS. GROSS: Hacking is pretty much taking something apart and figuring out how it works. When you open up the hood of your car and you tinker around in there, you are hacking your car. Hacking is simply exploring, learning, educating yourself, being curious about something, taking it apart, tinkering here and there, figuring out how it works. It, in and of itself, is not illegal or should be seen as somehow inappropriate activity.

Look at reverse engineering. Most of why this country is so strong right now is because of our technology development, is because we have hacked through technology, figured out how it works, figured out a way to make it better, and then built a new tool as a result. That is hacking.

QUESTIONER: I have a question, and also a comment. I am Amy Hyde-Juarez. I work at America Online (hereinafter "AOL"),¹⁴⁶ so I am coming to this with a different perspective, which is not so much from the publishing perspective or from the consumer's perspective, but from the content-distribution network side.

I think we are faced with a dangerous situation where you have publishers who can decide what digital encryption technology they want to use, which can force not only the consumer into an end-user application, but also the content-distribution networks into using certain types of technology—servers, protocols—for propagating that type of digital rights management technology across networks.

So I do not know how legislation can necessarily help that, or whether or not the DMCA addresses that at all, but I think there is a danger for those who own the copyrights to then dictate to the content-distribution networks what they can use. Not to use Microsoft as an example, but their digital management technology forces you to use NT servers, for example. So it can be very limiting, not only to the consumer, but the distribution networks as well.

¹⁴⁶ The views expressed by Amy Hyde-Juarez are individual opinions and are not necessarily those of America Online.

MR. SMITH: Is not your company under an antitrust investigation initiated now by the FTC for their particular music distribution system, that Warner Brothers, which is a division of AOL, is trying to do exactly what you are describing?

MS. HYDE-JUAREZ: Yes. I think that there are a lot of different technologies that are used right now for the distribution of digital assets. Clearly AOL, as being a company within AOL Time Warner, which also owns a lot of copyrights, we are working closely to figure out what works. It is a complicated issue, and that is why I bring it up. How do we protect not only the copyright holders, but the content-distribution networks and the consumers and give them choice?

MR. SMITH: I do not think this is a legal issue. I do not think there is anything that mandates DRM (digital rights management) right now. I defer to others that are more knowledgeable than me, but I do not think there is any mandate that you have to recognize DRM that passes over your network if your network does not recognize it. Now you may, for a competitive reason, want to pass it through because your customers want access to it, but I do not think you have to.

MS. GROSS: The problem that you raise is a really important one. It is that the DMCA is able to use technological means to turn individual rights into product features which can be disabled at the whim of a publisher, things like make a copy of a page for your school report, you know, the list goes on and on of all these things, lawful copying, lawful uses, that we have always had both the right and the ability to engage in, that have been seen as socially important, beneficial to society, but now these are suddenly things that can be disabled at the whim of a copyright holder. That is the problem: there is no one really representing the public side of the copyright bargain here, there is no one standing up for the public's rights, the public's interest.

QUESTIONER: I am Chris Pennisi, a first-year associate at Hopgood & Calimafde and former editor of the *Fordham IPLJ*. The question I have is directed to the panel, but really to Congress. The DMCA kind of is an anomaly, in that it unifies creation of a tool to

infringe a copyright and the actual act of doing the infringement, which, other than its title, seems to come only in that it is in the digital realm.

I do not think anyone would argue that Xerox or Canon is liable for any of the copyright infringing that goes on, probably on a daily basis, in libraries all across America. And yet here we are holding one scientist responsible for creating a tool. I think if the *Betamax* case¹⁴⁷ came out today under the DMCA, it would probably be going the other way.

So I would just like to put the question out: why should there not be a more intelligent intent requirement in this statute?

MR. SMITH: I want to say something about how the *Betamax* case¹⁴⁸ would have gone “the other way.” If applied to circumvention rather than contributory infringement, I think definitely it would have gone the other way; it was part of the intent of this statute that the *Betamax* result not be the rule. The Court in the *Betamax* case did not say that the result that it mandated—no contributory infringement—was the result that was automatically required under the Constitution or anything like that.¹⁴⁹ Under the existing law at the time, the Court found that there was a substantial non-infringing use, and therefore they had to find for the defendant in that case.

The *Betamax* case was very much in the mind of Congress when they enacted this statute, and they clearly intended for that result not to be repeated with respect to circumvention.¹⁵⁰

MS. GROSS: I would suggest that everyone go read the legislative history and look at the comments by the congressmen in terms of what they thought they were enacting, and particularly from our current U.S. Attorney General, John Ashcroft.¹⁵¹ All throughout the legislative history they are saying, “I am willing to sign this bill

¹⁴⁷ See *Sony*, 464 U.S. at 417 (1984).

¹⁴⁸ *Id.*

¹⁴⁹ *Id.*

¹⁵⁰ See S. REP. NO. 105-190, at 2 (1998); H.R. REP. NO. 105-551, pt. 2, at 38-40 (1998).

¹⁵¹ See, e.g., 145 CONG. REC. S11,887 (daily ed. Oct. 8, 1998), available at <http://www.hrrc.org/2281ConfReptAshcroftOct8.pdf>.

today, to vote for this bill, because I have been reassured that *Betamax* remains the law of the land,” and that is a quote.¹⁵²

MR. SMITH: *Betamax* is the law of the land with respect to copyright infringement.¹⁵³ This is not a case of copyright infringement. *Betamax* is still the law.¹⁵⁴

MR. FEDER: I know that in the meetings that I was a part of during the drafting phase of the DMCA, one of the early things that we considered was whether we could move forward without legislation at all. The government experts on this subject area were in pretty much unanimous agreement that because of the *Betamax* threshold,¹⁵⁵ the substantial non-infringing use test, that we could not move forward on the basis of just copyright protection because that would not constitute adequate and effective protection against circumvention, and therefore there had to be something in addition and there had to be a tightening of that standard, which is why you have those three criteria in the law: the intended purpose, or the intent for which it was created; the absence of commercially significant uses that are not for circumvention; and the purpose for which it is marketed.¹⁵⁶

MR. BURTON: Could I ask you, in light of that, ask you the question—and I would like to be enlightened on this; I mean that—why Congress decided not to prohibit circumvention of usage controls and did as to access controls? What was the reason for that?

MR. FEDER: Well, simply stated, unauthorized use can be a fair use. Unauthorized access is not something that is rendered non-infringing by the fair use doctrine.¹⁵⁷ To put it in terms of an analogy, if you copy a manuscript, that could be a fair use. If you break into my office and steal a manuscript, gain unauthorized access to it, fair use will not forgive you for that conduct. Fair use presupposes authorized access.

¹⁵² *Id.*

¹⁵³ *See Sony*, 464 U.S. at 417 (1984).

¹⁵⁴ *See* 144 CONG. REC. S11,888 (Oct. 8, 1998) (statement of Sen. Ashcroft).

¹⁵⁵ *Id.*

¹⁵⁶ *See id.*

¹⁵⁷ *See Definition of Fair Use*, *supra* note 56.

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 853

MR. BURTON: But then why is there a prohibition against a tool that can be used to enable just what you said, which is a fair use under the usage rights? Explain that to me. Why is the tool that could enable the fair use that you just described, why is the making of that tool prohibited or criminal?

MR. FEDER: Because there is no tool that can just do fair use.

MS. GROSS: This idea that tools are not able to distinguish between what is a fair use and what is not a fair use, and therefore we just have to outlaw fair use altogether, somehow gets short shrift.

MR. FEDER: We have not outlawed fair use.

MS. GROSS: But we have overlooked the important constitutional underpinnings involved in fair use.

MR. SMITH: Can I ask a question? Let me see if I can refine this in some way. If the defendant in the case had developed a tool for his or her own personal use, so, in other words, that person purchased an e-book from Adobe, then got the Adobe eBook Reader, then developed this tool and used it themselves, would that not violate the statute?

MR. LEHMAN: It might violate the manufacture part. But I do not know. That is a tough one. It depends on if you do it just for yourself. It depends on if the wording of the statute presupposes this kind of commercial activity, I think.

MS. GROSS: Yes, manufacture, which means “make.”

MR. FEDER: And for purposes of commercial advantage or private financial gain.¹⁵⁸

MR. LEHMAN: Right.

MS. GROSS: For the criminal provisions that is true, but for civil liability all you have to do is make the tool.

MR. LEHMAN: Oh, I am not so sure.

MR. FEDER: I don't think that is a correct interpretation because

¹⁵⁸ See *DMCA*, *supra* note 1.

that would essentially read out the distinction between conduct and manufacture and trafficking.

MS. GROSS: That is the problem we have.

MR. FEDER: And so I think it is just a simple matter of statutory interpretation. You have to assume that manufacture includes some commercial component.

MR. BURKE: We have another question from the floor.

PROFESSOR COENRAAD VISSER: Thank you, Chair.

I just want to take us back to the source of the DMCA, and that is the WIPO Copyright Treaty.¹⁵⁹ Many of the arguments we hear now are arguments which were raised during the Diplomatic Conference preceding the adoption of the Treaty, that the devices cannot distinguish between legitimate and illegitimate use, the shrinking of the public domain, all of that. That is why the wording of that particular provision in the Treaty is specific.¹⁶⁰ It is much more limited than the wording of the DMCA. It does not strike at manufacturing devices; it strikes only at the actual circumvention.

If you go and read the proceedings of the Conference, when the group that I was the spokesperson of introduced the wording of that act, it specifically said that the wording of the Treaty is introduced in the way in which it is, and in that limited way, because of the problems of the shrinking public domain, which will be against the interest of user groups, because of the problems that you cannot have a device where the device itself can distinguish between the different devices.¹⁶¹

¹⁵⁹ See *WIPO Copyright Treaty*, *supra* note 43.

¹⁶⁰ See *id.*

¹⁶¹ See WIPO Second International Conference on Electronic Commerce and Intellectual Property, Sept. 19-21, 2001, available at <http://ecommerce.wipo.int/meetings/2001/conference>.

2002] *SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS* 855

So the United States went far beyond what was its obligation in terms of the WIPO Copyright Treaty, and my question then is: why did the United States do that?

MR. SMITH: So did Europe, so did Japan and so will eventually every other country. Let me just speak to that because I think you raise a very good point.

The extension of this statute to devices from acts depends on national governments and how they interpret “adequate legal protection and effective legal remedies,” et cetera. The United States made its decision. Congress decided we have to get at not just the act of an individual, we have to get to the device.

In fact, the language that is in the Treaty was originally drafted by the copyright community as a result of negotiations with the Consumer Electronic Manufacturers Association,¹⁶² who were very concerned that the VCR and all the new products that they would manufacture might be called circumvention devices. The generality of the language was to defer to the future exactly how the statute would be crafted, and this was kind of compromise language that was agreed on.

The African Delegation introduced that language, but I think if you want to go to the legislative/negotiating history of it, the language was developed by the European, Japanese, and American consumer electronics industry plus all the content community, and it was clearly intended when that language was drafted originally, before it went into the Treaty, that it would cover devices, clearly intended that it would cover devices.¹⁶³

MR. FEDER: I think there are two problems with focusing just on end-user conduct. One, it is not effective. Copyright law already permits you to go after end-users who commit copyright infringement.

¹⁶² Information about the Consumer Electronic Manufacturers Association is accessible online at <http://www.cemaonline.com/>.

¹⁶³ See WIPO Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, Dec. 2-20, 1996, available at http://www.wipo.int/news/en/index.html?wipo_content_frame=/news/en/conferences.html.

The reason why we are considering all this technological mumbo-jumbo is because that does not work. You cannot detect it, you cannot chase these people down, you cannot recover anything when you get them. So there is no adequate and effective way of solving the problem just by going after end-users.

The other problem is: do you want the government chasing after end-users? Do you want the copyright owners chasing after end-users and penalizing that kind of conduct? I think, from a policy perspective, that is a less desirable way to go than moving back to what Bruce described as a choke point, the people who are in the business and profiting from providing the means for people to engage in this conduct.

MR. SMITH: We have to stand back and see what is the purpose of these laws. It is not to be mean to people or anything like that. It is to protect the rights of authors and publishers so that we can have a thriving business in the publication of ideas in this country.

MS. GROSS: The problem is it goes farther than protecting the rights of authors. It infringes upon the rights of the public. We would like to see a balance.

MR. SMITH: How could we? If this gentlemen were permitted to sell this device to millions of people, how in the world, as a practical matter, could we effectively have a market in electronic books?

MR. BURTON: Is there any law that you are aware of that makes it illegal to manufacture lock picks?

MR. SMITH: It is illegal to possess burglar tools.¹⁶⁴

MR. BURTON: With the intent to do an illegal act. It is never—there is no statute in the United States that makes the mere possession or the mere manufacture of a burglar tool—illegal. None.

MR. SMITH: There is one now. There is one now in this area, and we have it, and your client is stuck with it, and he is getting prosecuted under it.

¹⁶⁴ See, e.g., N.Y. PENAL CODE § 140.35.

2002] SYMPOSIUM: GLOBAL INTELLECTUAL PROPERTY RIGHTS 857

MR. BURTON: And if you can prove it unconstitutional, if you can say that Congress had no authority to pass this law, then it will be struck down.

MR. SMITH: Well good, then I can go home.

MR. BURKE: We have time for one more question.

QUESTION: My name is Chris Stambaugh. I am a second-year student and a staff member of the *Fordham IPLJ*.

I was just wondering, with the intent of the DMCA to prevent copyright infringement, how successful it has been and how successful you expect it to be? Whether it is right or it is wrong, I personally do not see it working. I do not see infringement slowing down.

MR. SMITH: I think it has been phenomenally successful. Look at the cases that have come up. This is not *Betamax* all over again.¹⁶⁵ The copyright owners have won virtually every single piece of litigation.

MS. GROSS: Yet the information is still out there, so it has been useless.

MR. SMITH: Standards are being put together for the digital age which will respect the rights of authors and publishers and create a wonderful new business of the dissemination of ideas in the digital age. That is what is happening. You do not have a lot of experience yet. The *DeCSS* case¹⁶⁶ was the first big circumvention case, and the copyright owners won under the statute. If the Norwegian hacker had been in the United States, he would probably be subject to criminal prosecution right now, but he was not.

MS. GROSS: I think it is sort of a fantasy to imagine that because the DMCA is law that this information is not going to be disseminated and the effects of what these people are trying to prevent against are going to somehow be precluded. In all of these cases where the DMCA has been invoked so far, the information that

¹⁶⁵ See *Sony*, 464 U.S. at 417 (1984).

¹⁶⁶ See *Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

they are trying to squelch is everywhere, continues to be everywhere, so their idea that, “Yes, it’s working, we are protecting our interest,”—it makes no sense because what the government is able to go after is a particular individual and put him in jail, but they are not able to prevent people from having access to this information. And so I do not see how the DMCA gets them what they want in that respect.

MR. SMITH: But will it deter? That is the question. Will it deter future conduct, people from making these kinds of devices in the future, if they know that it is a crime?

MR. LEHMAN: For the record, I want to make it clear that I totally disagree with the RIAA’s position in the *Felten* case¹⁶⁷ and completely distinguish that from the case that we are discussing here.

MR. SMITH: You know, RIAA is a member of my organization, and I am not speaking for them now, I am speaking only for myself. Somebody at RIAA sent a letter, and I think now everyone is backing away from this because they realize that it has very significant First Amendment elements and nobody wants to go after Mr. Felten. Everybody has written letters to the court saying, “Sorry, we did not mean to write that letter. We do not want to prosecute Mr. Felten.”¹⁶⁸

MR. BURKE: On that note we have to end.

MR. GALBRAITH: I am Kevin Galbraith, Editor-in-Chief of the *Fordham IPLJ*. Before you go, I want to sincerely thank all of our panelists and our audience for an excellent series of discussions. Thanks also to Natalie Suhl and Amy Feinsilver, and most of all to our Symposium Editor Margaret Ross, who conceptualized this conference and then worked tirelessly to make it successful.

¹⁶⁷ See *Felten v. Recording Indus. Ass’n of Am.*, No. CV-01-2660 (D.N.J. filed 2001), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

¹⁶⁸ The letters to Judge Brown from Verance, RIAA, and SDMI are accessible online at http://www.eff.org/Legal/Cases/Felten_v_RIAA/felten_legal_documents.html.