John T. Egley
Michael Matoba
Iram Parveen Bilal
Meng-Meng Fu
United States Attorneys,
LoyoTech Division

Arif Alikhan
Jim Spertus
United States Attorney's Office

Attorneys for the Prosecution
United States of America

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Prosecution, vs. DR. BALTIMORE, PROFESSOR SUN-DANCE LAW, JOHN JOHNSON, AND THE CALIFORNIA INSTITUTE OF TECHNOLOGY, Defendants.	Case No.: MHP-04-9999 SUMMARY OF EXPERT STATEMENT OF C. BRADLEY HUNT Date: May 21, 2004 Time: 2:15 pm Courtroom: Beckman Auditorium

The United States of America respectfully submits this Summary of Prosecution Expert C. Bradley Hunt pursuant to the court's order setting a hearing date for May 21, 2004.

QUALIFICATIONS

1. My name is C. Bradley Hunt. I am currently the Senior Vice President and Chief Technology Officer for the Motion Picture Association of America, Inc. I have a Bachelor of Science degree in Chemical Engineering from the Rose-Hulman Institute of Technology and an M.B.A. degree from the William E. Simon Graduate Business School at the University of Rochester. A copy of my curriculum vitae is attached as Appendix A.

2. I have worked in the motion picture and television industry for over twenty-five years. I currently work closely with the seven member companies that make up the MPAA in providing guidance on technology issues and policymaking related to copy protection, anti-piracy, Internet security, and digital cinema. I have also publicly spoken at a variety of conferences and seminars on the topics of content protection, piracy, and the broadcast flags.

3. My career experiences have ranged from research and development of motion picture film stocks to executive management of HDTV tele-cine and digital film post-production hardware businesses. I have also worked in the video post-production service industry where I helped establish one of the early DVD pre-mastering and MPEG compression service facilities in Los Angeles.

4. The Motion Picture Association of America is a non-profit trade association consisting of the seven major studios in Los Angeles. I am a Fellow of the Society of Motion Picture and Television Engineers and am also on the Technical Advisory Board of the University of Southern California Entertainment Technology Center.

5. In 1999, I joined the MPAA as chief technology officer and established the MPAA Office of Technology. In one of my important areas of responsibility, I worked closely with the studio technical, legal, and commercial executives on copy protection related activities. These activities included facilitating discussions with content protection technology developers on the technical specifications and non-economic licensing terms associated with their content protection technologies. For example, I have worked closely with the member companies in their negotiation with the 5C

companies on the Digital Transmission Content Protection technology, with the 5C companies on the Content Protection for Recordable Media technology, with Intel on the High-Bandwidth Digital Content Protection technology and with the DVD Copy Control Association on the DVD Content Scrambling System technology. "5C"stands for a group of five companies, Sony, Matsushita, Intel, Toshiba, and Hitachi.

6. In late 2001, I participated for six months in the Broadcast Protection Discussion Group, which was a sub-group formed by the cross-industry Copy Protection Technical Working Group. I was actively involved in the discussions of the functionality of the broadcast flag solution and the related content protection technologies necessary to assert downstream protection of digital broad-cast television content from unauthorized redistribution. I have also been involved in the drafting of MPAA filings with the Federal Communication Committee on the FCC Digital Broadcast Content Protection proceedings.

CLAIM 1: EFFECTIVENESS OF DRM/CCI DEVICE WITHIN THE DMCA

7. Digital coding systems consist of bits. The term "bit" is an abbreviation for binary digit. Each bit contains one of two symbols, either a 0 or 1. Sequences of bits are used to represent all kinds of digital data ranging from music and movie files to ordinary computer programs. One of the benefits of digital information is the ease with which it can be copied and shared. However, this benefit also enables individuals to copy and redistribute digital content easily, without regard to the rights of others, such as the copyright holders who may own the digital content.

8. To prevent the breach of copyright, companies have created Digital Rights Management ("DRM") systems, which use encryption technology to securely protect digital content and to bind the set of digital usage rights associated with the content. There are several different DRM tech-nologies used to control copying and redistribution of digital content. These DRM or copy protec-tion technologies encrypt both the digital content and the embedded Copy Control Information

(“CCI”) associated with the content. The CCI is a set of bits that convey the digital usage permissions associated with the content stream. The CCI also specifies whether the content can be copied or not and whether the content may be digitally redistributed. Only devices that are manufactured under license from the DRM technology licensors will possess the necessary keys to gain access to the encrypted content. A DRM licensed device that receives encrypted content will be able to authenticate itself with the transmitting device in order to receive the keys necessary for decrypting the content and the embedded CCI, which it will obey. Unlicensed devices will not be able to authenticate themselves to the transmitting device and therefore will never be able to obtain the keys to decrypt and access the content stream.

9. The 5C companies, developed a link encryption technology called Digital Transmission Content Protection “DTCP” in order to further protect their rights. This DRM technology protects the content flowing across a digital connection between a “source” device and a “sink” device. Device manufacturers who want to build devices incorporating the 5C DTCP technology must sign an Adopter License, which is issued by the Digital Transmission License Administrator (DTLA). Adopters, who are companies that sign a DTCP license with DTLA, can incorporate the confidential digital certificates and cryptographic ciphers into their devices or software, in order to encrypt and decrypt digital content using the 5C DTCP technology. However, they are legally obligated not to reproduce or sell the confidential information associated with the 5C DTCP technology (section 5.6, DTLA agreement). A 5C DTCP source device generates a session key for encrypting the content and the embedded CCI being transmitted across the digital interconnect. This session key is changed every 2 minutes in order to provide greater robustness against brute force attacks of the encryption. Brute force attacks are attempts by a non-authorized user to gain access to the protected content by trying every possible combination for the session key. This means that any brute force hack of the 5C DTCP technology will reveal a single session key that can unlock only 2 minutes of protected content.

10. Therefore, the purpose of DRM technology is to prevent the illegal access and usage of encrypted data by unlicensed individuals. It is effective because it prevents ordinary users without licenses from building devices that can decrypt and gain access to the protected content using technical skills and technology commonly available to individuals.

CLAIM 2: CIRCUMVENTION OF THE DRM

11. 5C DTCP technology has been implemented in many commercially available consumer electronics devices, including ATSC Digital TV receivers, Satellite TV Receivers, Digital Cable set top boxes, and Digital VHS recorders. For example, the 5C DTCP technology can be used to protect digital content flowing across an IEEE 1394 interconnect between a Satellite TV receiver and a Digital VHS high definition television (HDTV) recorder. 5C DTCP technology encrypts the digital content and the embedded CCI using 56-bit encryption. There are two ways of cracking the encryption. First, it can be done by brute force, or trying every possible solution or key. In a 56-bit encryption, there are 2^56 (7.2 x 10^16) possible combinations, with only one correct solution. It is statistically unlikely for an ordinary individual using a standard computer to find this solution. But since the 5C DTCP content encryption key is changed every 120 seconds, any successful brute force attack will only expose 120 seconds of the content. The second way of cracking the encryption can be done by finding an algorithm, or mathematical solution, that limits the field of search. Currently, no such "loopholes" have been discovered related to the encryption cipher used in the 5C DTCP technology.

12. After reviewing the final facts of this case, I have familiarized myself with the Johnson case. Johnson's method of circumventing the 5C DTCP technology did not exploit any weaknesses in its underlying encryption technology. Rather, he used a web site to organize a distributive-computing brute force attack that tries every possible solution to the encryption using massive amounts of distributed computing power. Since Johnson was previously able to circumvent a 56-bit encryption,

his method would be able to break the 56-bit encryption used by the 5C DTCP technology. However, Johnson was only able to stage these brute force encryption technology attacks by constructing a web-based collaborative decryption system that combined the idle processing power of many individual computers linked over the Internet. But even with a successful brute force attack of the 5C DTCP technology, the unauthorized user would only gain a single decryption key, allowing him access to a mere two minutes of protected content. Thus, the 5C DTCP technology is still an effective copyright protection measure since it changes its content encryption key every 120 seconds.

13. Hence, the current 5C DTCP technology is a robust system that successfully prevents circumvention of the encryption by people with ordinary technical skills and computing power. This system can only be circumvented by knowledgeable professional technicians with massive processing power who approach the DRM with the intent of illegally cracking the encryption. Thus, even someone with Johnson's skill, as well as an ordinary user, would be unable to circumvent the technological protection measure without combined computing power. Johnson was only able to undermine this effective encryption system by providing a complicated program for decryption that allowed users with insufficient knowledge and meager processing power to access decryption keys illegally.

CLAIM 3: COST-BENEFIT ANALYSIS OF CURRENT DRM vs. POSSIBLE ALTERNATIVES

14. The current 5C DTCP technology is an effective technological protection measure that prevents ordinary users from unauthorized copying and redistribution. The only possible cost to consumers is posed by skilled technicians carrying out illegal hacks that are then widely disseminated to consumers. When the technology used to circumvent a technological protection measure is shared, as in this case, the cost of the copyrighted media to the ordinary, law-abiding consumer more than likely will increase. It is very challenging and costly to design DRMs to defend against

such professional, organized attacks, because even if the most advanced and complicated technology is used, it can still always be hacked in the future as long as certain expert hackers are intently working to circumvent it.

15. Possible alternatives to the DRM should only be considered if ordinary users are able to individually circumvent the current DRM. The cost of developing and implementing these alternatives is high. For example, using longer content encryption key lengths would cause incompatibility problems with existing 5C DTCP devices and would increase costs in all consumer devices. However, since the current 5C DTCP technology is effective in preventing ordinary users from circumventing it, the implementation cost associated with using longer key lengths or more advanced cryptographic algorithms seems unnecessary. Hence, employing more robust technologies is not very cost effective for the digital industry. This is especially true if the law continues to overlook the efforts of hackers such as Johnson who combine computing power in order to organize brute force attacks to reveal a DRM's decryption keys. The duty of preventing successful hacks by even the most knowledgeable professional technicians should not be imposed upon device manufacturers and digital media providers, but in fact should be tackled by legal intervention.

Appendix A: Curriculum Vitae

NAME. C. Bradley Hunt

TITLE. Senior Vice President and Chief Technology Officer.

Motion Picture Association of America, Inc

ADDRESS. 3563 Twin Lake Ridge

Westlake Village, California 91361

TELEPHONE. 1-818-706-0580

email: cbhunt1@earthlink.net

EDUCATION

B.Sc., Chemical Engineering - ROSE-HULMAN INSTITUTE OF TECHNOLOGY, Graduated with High Honors in 1976.

M.B.A., Executive Development Program – WILLIAM E. SIMON GRADUATE SCHOOL OF BUSINESS ADMINISTRATION, UNIVERSITY OF ROCHESTER, Graduated with High Honors in 1990.

PROFESSIONAL EXPERIENCE & ACCOMPLISHMENTS

1999 - present Senior Vice President, Chief Technology Officer

Motion Picture Association of America, Encino, California

• Responsible for leading the consensus-building process and policy-making with the seven major motion picture studios in technology, legal licensing, and legislative aspects associated with content protection, digital rights management, digital cinema, DVD, and digital television broadcasting.

• Created the MPAA Office of Technology and hired its engineering staff to support the studios through participation in international standards activities, operation of a copy protection compliance-testing laboratory, involvement in anti-piracy operations, and management of outside research projects.

1998 - 1999 President & CEO

Cintel Incorporated, Valencia, California

• Refocused the US-based manufacturing and product development areas and launched two US product development programs, a new HDTV telecine and a new digital film scanning IRIX software utility.

• Reorganized and strengthened the North American customer service organization resulting in significant improvements in customer support quality levels and response time.

1996 - 1998 Senior Vice President, Technology

All Post Incorporated, Burbank, California

• Prepared capital equipment budget, identified new technology investments, and created an HDTV participation strategy for this multi-million dollar film restoration, audio, and video post company.

• Established and grew the company's digital MPEG compression and DVD premastering division providing services to the DVD-Video, DVD-ROM, CD-ROM, and video server markets.

1995 - 1996 Director of Operations, Digital Motion Imaging

Eastman Kodak Company, Rochester, New York

• Worldwide management and P&L responsibility for Kodak's Digital Motion Imaging manufacturing, customer service and support, supply chain logistics, training, and international sales organizations. Managed 50 people based in four locations around the world with an annual budget of $20 million.

• Initiated a cost reduction program that reduced the manufacturing cost of Kodak's Cineon Lightning Laser Film Recorder product by 66% and improved product reliability and serviceability.

1991 - 1995 European Region Sales & Business Development Manager

Motion Picture & Television Imaging, Eastman Kodak Company, London, UK

• During a London assignment, recruited and managed a 12-person, pan-European sales, marketing, and service organization to launch the Cineon Digital Film System business. Exceeded European sales goals every year and achieved an annual revenue growth rate exceeding 200% for three years.

• Created the business plan and was responsible for site selection, build out, and start up of the Cinesite Digital Film Center in London and the Kodak Cinemas AO showcase theater in Moscow, Russia.

• Negotiated a multi-million dollar HDTV Imaging Head development and supply contract with Philips Broadcast Television Systems leading to the introduction of the Philips Spirit Datacine film scanner.

1987 - 1991 Director, Advanced Technologies Planning

Motion Picture & Television Imaging, Eastman Kodak Company, Rochester, NY

• Responsible for creating and selling top Kodak management on a 5-year Digital Imaging strategy which led to the company's launch of its Digital Motion Imaging (DMI) business, which included the Cineon Digital Film System and the Cinesite digital film service businesses.

• Successfully negotiated partnership contracts with many diverse companies such as Rank Cintel, BTS, Silicon Graphics, Lucasfilm, and Ampex in the development and launch of the DMI business.

1985 - 1987 Marketing and Product Planning Coordinator, Electronics

Motion Picture & Audiovisual Markets, Eastman Kodak Company, Rochester, NY

• Created the product plans and successfully negotiated the Japanese sourcing of Kodak Professional 8mm video recorders from Matsushita Electric and Color LCD video projectors from Seiko Epson.

• Produced innovative marketing plans, sales materials, and packaging designs instrumental in growing Kodak's professional videotape worldwide market share to 5% in two years.

1981 - 1985 Sales & Engineering Representative

Motion Picture & Audiovisual Markets, Eastman Kodak Company, New York, NY

• Worked closely with 19 optical houses to train them in the use of the Laboratory Aim Density printing exposure control system, which resulted in screen quality improvements in their optical film effects.

1980 - 1981 Motion Picture Product Marketing Specialist

Motion Picture & Audiovisual Markets, Eastman Kodak Company, Rochester, NY

• Developed the concept and pioneered the introduction of Kodak's Telecine Analysis Film that is in use today as a tool to improve telecine setup and the quality of film-to-tape transfers.

1976 - 1980 Photographic Engineer

Motion Picture Products Group, Eastman Kodak Company, Rochester, NY

• Responsible for the research and development of new motion picture film products and processes, including Eastman Color Intermediate II Film 5243, which won an Academy Award.

• Developed and published an innovative method for restoring faded color motion picture film prints, which won the SMPTE Journal Award.

PROFESSIONAL SOCIETIES & HONORS

Rose-Hulman Institute of Technology Distinguished Young Alumnus Award – 1996

Fellow of the Society of Motion Picture and Television Engineers (SMPTE)

Executive Member of the Technology Council of the Motion Picture and Television Industry

Member of the Inter-Society Digital Cinema Advisory Group

Member of the Technical Advisory Board of the University of Southern California Entertainment Technology Center Digital Cinema Laboratory

Member of the Digital Video Broadcasting Copy Protection Technical Module

Participant in the SMPTE Digital Cinema Engineering Study Groups

Participant in the Copy Protection Technical Working Group

Over 10 technical papers published in the SMPTE Journal and other trade publications

HIGHLIGHTS OF QUALIFICATIONS

-- Over 25 years experience and contacts in the motion picture and television industry worldwide.

-- Skilled in identifying and developing new, high technology business opportunities.

-- Experienced in managing international partnerships and alliances with multinational corporations.

-- Effective at promoting and selling new technology-based products and services.