

1 John T. Egley  
2 Michael Matoba  
3 Iram Parveen Bilal  
4 Meng-Meng Fu  
5 United States Attorneys,  
6 LoyoTech Division

7 Arif Alikhan  
8 Jim Spertus  
9 United States Attorney's Office

10 Attorneys for the Prosecution  
11 United States of America

12 UNITED STATES DISTRICT COURT  
13 WESTERN DISTRICT OF CALIFORNIA

14 UNITED STATES OF AMERICA, ) Case No.: RL-04-9999  
15 Prosecution, )  
16 vs. ) MEMORANDUM OF POINTS AND  
17 DR. DANIEL BALTIMORE, ) AUTHORITIES IN OPPOSITION TO  
18 PROFESSOR SUNDANCE LAW, JOHN ) DEFENDANTS' MOTION TO DISMISS  
19 JOHNSON, AND THE CALCULATING )  
20 INSTITUTE OF TECHNOLOGY, )  
21 Defendants. )

Date: May 21, 2004  
Time: 2:15 pm  
Courtroom: Beckman Auditorium

22 The United States of America respectfully submits this Memorandum of Points and  
23 Authorities in Opposition to Defendants' Motion to Dismiss pursuant to the court's order setting a  
24 hearing date for May 21, 2004.

**TABLE OF CONTENTS**

	<u>Page</u>
TABLE OF AUTHORITIES .....	iii
INTRODUCTION.....	1
STATEMENT OF FACTS .....	2
ARGUMENT.....	3
I. 5C Encryption Technology is Effective Within the Meaning of the DMCA at Controlling Access to Protected Material .....	3
A. The Legislative Intent Behind the DMCA Supports a Broad Interpretation of the Term “Effective” Such That Defendants Can be Found Liable .....	2
B. The Technological Protection Measure Used by the 5C Method of Encryption Successfully Prevents Circumvention of the Encryption by People With Ordinary Technical Skills and Computing Power .....	6
1. 5C encryption is effective because it prevents the vast majority of the population from accessing copyrighted material and there are no readily available cost-effective alternatives .....	6
2. 5C encryption, in the ordinary course of its operation, requires the authority of the copyright owner to gain access to the protected work.....	7
II. The First Amendment to the United States Constitution does not Prevent Enforcement of the DMCA.....	8
A. Johnson’s Circumvention Program is not Speech Within the Meaning of the First Amendment .....	8
B. Even if the First Amendment Protections Apply to Material Covered by the DMCA, Such Material Would be Commercial Speech Which Congress can Constitutionally Regulate.....	9
1. Since the government regulation is content neutral, the regulation of speech is subject to the lesser standard of intermediate scrutiny .....	9
2. Even if the court applies strict scrutiny to the regulation, the regulation of speech does not violate the First Amendment .....	10

1 III. Vicarious Criminal Liability Need Not Apply to Sundance Law, Caltech, and  
2 Dr. Baltimore Because all of the Defendants Directly Violated the Digital  
3 Millennium Copyright Act and Caused Circumvention of Digital  
4 Management Technology ..... 11  
5  
6 A. Sundance Law, John Johnson, Dr. Baltimore, and Caltech Willfully  
7 Violated 17 U.S.C. § 1201 for Commercial Advantage and Financial  
8 Gain When the Class Website Enabled Internet Users to Obtain  
9 Decryption Keys to Circumvent 5C Technology and are Culpable  
10 Under 17 U.S.C. § 1204..... 11  
11  
12 B. Professor Law, Dr. Baltimore, and Caltech can Also be Found to  
13 Willfully Violate 17 U.S.C. § 1201 for Commercial Advantage and  
14 Financial Gain When They Have Actual Knowledge of Infringing  
15 Activities and They Refuse to Remove it From Their System ..... 15  
16  
17 IV. The Defendants are Criminally Liable for Willfully Violating 17 U.S.C. §  
18 1201(b)(1) for Trafficking in Circumvention Technology for Commercial  
19 Advantage or Financial Gain. .... 16  
20  
21 V. Sundance Law, Caltech, and Dr. Baltimore are Criminally Liable for Aiding  
22 and Abetting the Criminal Circumvention of Digital Management  
23 Technology That is Used to Protect Copyright Infringement..... 17  
24  
25 A. Sundance Law, Caltech, and Dr. Baltimore had the Ability to Control  
26 and Regulate the Website With the Computer Program That Allowed  
27 Circumvention of Digital Rights Management..... 18  
28  
29 B. Sundance Law, Caltech, and Dr. Baltimore gained a financial benefit  
30 from the circumventing technology ..... 19  
31  
32 CONCLUSION ..... 22

**TABLE OF AUTHORITIES**

Page(s)

**Supreme Court Cases:**

Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985) ..... 13

Inwood Laboratories v. Ives Laboratories, 456 U.S. 844 (1982) ..... 17

Perry Ed. Assn. v. Perry Local Educators’ Assn., 460 U.S. 37 (1983)..... 10

Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984)..... 18

Transworld Airlines, Inc. v. Thurston, 496 U.S. 111 ()..... 12

Turner Broad Sys., Inc. v. FCC, 512 U.S. 622 (1994)..... 9,10

United States v. O’Brien, 391 U.S. 367 (1968) ..... 9

Ward v. Rock Against Racism, 491 U.S. 781 (1989) ..... 10

**Federal Court Cases:**

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)..... 13,15,16,19

American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1994)..... 14

Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004)..... 19

Fonovisa Inc. v. Cherry Auction, Inc., 76 F.3d 261 (9th Cir. 1996)..... 12,17,18

Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d  
1159 (2d Cir. 1971)..... 17,19

Lexmark Int’l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943  
(E.D. Ky. 2003)..... 12

Sega Enters Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal.1994)..... 14

United States v. Elcom, Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002)..... 9,10,16

Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001) ..... 4,8

Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y.  
2000) ..... 8

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Worldwide Church of God v. Philadelphia Church of God, 227 F.3d 1110  
(9th Cir. 2000)..... 13

**Statutes:**

17 U.S.C. § 101(a) ..... 14  
17 U.S.C. § 506 (a) ..... 12  
17 U.S.C. § 1201..... 3,4,7,12,13,16  
17 U.S.C. § 1202..... 11,12  
18 U.S.C. § 2(a) . § 1202 ..... 17,18

**Constitutional Provisions:**

U.S. Const. Art. I ..... 8

**Law Review Articles:**

Joseph Liu. Symposium: The Law and Technology of Digital Rights Management, 18 Berkeley Tech. L.J. 501 (Spring 2003) ..... 5  
Bonnie Schriefer. Comment: “Yelling Fire” and Hacking, 71 Fordham L. Rev. 2283 (April 2003). ..... 5

1 **INTRODUCTION**

2 This case is about theft and technological piracy. Defendants have all violated the  
3 provisions of the Digital Millennium Copyright Act of 1998 (“DMCA”), Congress’ response to  
4 the growing threat posed by these twenty-first century technological pirates. Much like the pirates  
5 of old that razed towns and wrecked havoc on the shipping industry, people seeking to circumvent  
6 technological protections measures are the new pirates of the twenty-first century. Both species of  
7 pirates are interested in the destruction of property and in the enrichment of their own coffers.  
8 Instead of riding the waves of the open seas, these new pirates surf the waves of the Internet.  
9 Instead of gold and precious gems, these pirates acquire valuable copies of movies, software,  
10 music, and other protected intellectual and digital property. However, the weapons of these  
11 twenty-first century pirates are more destructive than their predecessors as they have traded in  
12 their pistols and cannons for computers and electronic devices designed to gain access to protected  
13 material. The reach of this new breed of pirates is often world-wide as they are easily able to  
14 distribute their pirated wares of music, movies, and software to anyone with a computer. These  
15 pirates must be stopped and the filing of this indictment is the opening salvo in a battle that will  
16 have far-reaching consequences for those seeking to protect their copyrighted material.

17 John Johnson, Dr. Baltimore, Professor Sundance Law, and the Calculating Institute of  
18 Technology (“the Defendants”) have all been indicted for violating the DMCA. This brief is  
19 submitted in opposition to the Defendants motion to dismiss the charges filed against them.  
20 Defendants seek to dismiss the indictment on the grounds that the use of 56-bit encryption  
21 technology is no longer effective within the meaning of the DMCA, the First Amendment of the  
22 United States Constitution protects their activities, and that there can be no vicarious criminal  
23 liability based on the facts of this case. All of these arguments lack merit and persuasive force.  
24 Accordingly, this court should deny the Defendants motion to dismiss.

25 This criminal prosecution is important because of its potential deterrent effect on others  
26 interested and engaged in the activity of circumventing technological measures designed to  
27 prevent the unauthorized access and reproduction of copyrighted and other protected works. This  
28 court should bear in mind that a great deal of money is at stake since American companies

1 annually lose billions of dollars to piracy and have spent untold millions of dollars in an effort to  
2 protect their property rights. If the law cannot be used to protect their rights, than the development  
3 of new digital technologies will be irreparably halted.

#### 4 STATEMENT OF FACTS

5 During the Fall 2003 term at the Calculating Institute of Technology (“Caltech”),  
6 Defendant Law assigned the students in his Digital Protection class the task of devising and  
7 defeating technological protection measures (“TPM”). Each year, the class is divided into two  
8 halves with one group devising technological protection measures while the other half attempts to  
9 hack and circumvent the devised technological protection measures. One student, Dimitry Skylore  
10 (“Skylore”), developed an anti-copying system to protect digital content by embedding a  
11 complicated code in the digital content. Essentially, the embedded code would regulate access to  
12 the protected content and specify whether or not the underlying content could be copied. Skylore  
13 used 56-bit encryption to protect the digital content. 56-bit encryption is an powerful encryption  
14 such that significant computer power in addition to knowledge of computer technology is  
15 necessary in order to circumvent the system.

16 As a result of the assignment given to the 2003 class, a student, John Johnson (“Johnson”),  
17 came up with a way around Skylore’s technological protection measure. Defendant Johnson  
18 devised a distributed computational program that would allow a vast network of individual  
19 computers, linked over the Internet, to form one large super-computer. As a result of this  
20 program, Johnson was able to circumvent Skylore’s TPM within 24 hours. Defendant Johnson  
21 saw the lucrative potential for his circumvention technology and posted his program on a web site  
22 along with his resume, hoping that he would find employment as a computer consultant.

23 Professor Sundance Law (“Law”), also a defendant in this indictment, noticed that  
24 Johnson’s decryption program could be used to circumvent the “5C” Digital Transmission Content  
25 Protection (“DTCP”) technology being proposed for the FCC broadcast flag regulation (“5C”  
26 standing for the five companies that pioneered this technology). In fact, 5C DTCP technology was  
27 already being used by a wide variety of entertainment and consumer electronics companies in  
28 order to protect commercially distributed audio and video entertainment.

1 In order to prove his thesis that 56-bit encryption based TPMs were capable of being  
2 circumvented, Law posted a 5C DTCP encrypted movie on Johnson's web site. Within a day, the  
3 correct decryption key was found for the encrypted movie segment. Further clips were also posted  
4 on decrypted on the web site. As a result, these clips could be combined to make a clear copy of a  
5 protected movie.

6 Currently, word of Johnson's web site has spread quickly and the web site is experiencing  
7 heavy internet traffic from computers throughout the country. The Calculating Institute of  
8 Technology has refused to remove Johnson's web site and has refused to prohibit Law from  
9 teaching students how to circumvent TPMs. As a result, the United States of America is seeking  
10 criminal sanctions under the DMCA against Johnson, Law, Caltech, and Caltech's president, Dr.  
11 Baltimore.

### 12 ARGUMENT

#### 13 **I. 5C Encryption Technology is Effective Within the Meaning of the DMCA at** 14 **Controlling Access to Protected Material.**

15 The DMCA, found at 17 U.S.C. § 1201-1205, was Congress' way of legislating protection  
16 for copyright protection systems. Specifically, a person is prohibited from "circumvent[ing] a  
17 technological measure that *effectively controls access to a work* protected under this title." 17  
18 U.S.C. § 1201(a)(1)(A) (emphasis added). The term "effectively controls access to a work" is  
19 specifically defined in the statute. Under 17 U.S.C. § 1201(a)(3)(B), a measure effectively  
20 controls access to a work if the technological measure "in the ordinary course of its operation,  
21 requires the application of information, or a process or a treatment, with the authority of the  
22 copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). Thus, a technological  
23 measure is effective within the meaning of the DMCA if in the ordinary course of its operation it  
24 requires the authority of the copyright owner in order to access the work.  
25

26 This broad and expansive language in the DMCA deals with the case currently before this  
27 court. The 5C encryption which was circumvented by Johnson's technique, in the ordinary course  
28 of its operation, prevents people from accessing the protected material unless they have the proper

1 encryption key which allows them access to the digital content. Without the encryption key, users  
2 are denied access. A plain reading of the DMCA brings the facts of this case squarely within the  
3 province of the DMCA's regulations. As a result of its plain meaning, no construction of any  
4 statutory language is required. Furthermore, courts have specifically rejected attempts to narrowly  
5 construe the provisions of the DMCA. *See, Universal City Studios v. Corley*, 273 F.3d 429 (2d  
6 Cir. 2001) (narrow construction of DMCA cannot be inferred from 17 U.S.C. §1201(c)(4) which  
7 provides that this section does not enlarge or diminish any rights of free speech).

8 The DMCA also describes particular acts that are prohibited with broad and sweeping  
9 language. The DMCA specifically prohibits acts such as the:

10 manufacture, import, offer to the public provide, or otherwise traffic  
11 in any technology, product, service, device, component, or part  
12 thereof, that:

13 (A) is primarily designed or produced for the purpose of  
14 circumventing protection afforded by a technological measure that  
15 effectively protects a right of a copyright owner to a work protected  
16 under this title in a work or portion thereof;

17 (B) has only limited commercially significant purpose or use other  
18 than to circumvent protection afforded by a technological measure that  
19 effectively protects a right of a copyright owner to a work protected  
20 under this title in a work or portion thereof; or

21 (C) is marketed by that person or another acting in concert with that  
22 person with that person's knowledge for use in circumventing  
23 protection afforded by a technological measure that effectively  
24 protects a right of a copyright owner to a work protected under this in  
25 a work or portion thereof. 17 U.S.C. § 1201(b)(1)(A)-(C).

26 Here, Johnson has offered his circumventing device to the public by posting it on a web site that  
27 has been frequently visited by people all over the country. Johnson has clearly committed an act  
28 that is prohibited by the terms of the DMCA.

The DMCA also lays out extensive criminal penalties for persons that violate the Act  
willfully and for purposes of commercial advantage or private financial gain. 17 U.S.C. 1204(a).  
Violation of the DMCA is punishable by a fine of not more than \$500,000 and not more than 5

1 years imprisonment for a first offense, and not more than a \$1 million fine and not more than 10  
2 years imprisonment for each subsequent offense. *Id.* As discussed in Section III below, the  
3 Defendants qualify for these criminal sanctions because their conduct was willful and for the  
4 purpose of commercial advantage or private financial gain.

5 A. The Legislative Intent Behind the DMCA Supports a Broad Interpretation of the  
6 Term “Effective” Such That Defendants Can be Found Liable.

7 In addition to the already broad language employed by the statute, this court need not fear  
8 overreaching into areas that Congress did not intend to criminalize. Congress specifically  
9 addressed this potential problem by creating exceptions and exemptions for particular parties.

10 In particular, the DMCA has built into it a number of safe harbors for educational  
11 institutions and educational purposes. For example, section 1201(d) of the DMCA provides an  
12 exemption for libraries and educational institutions and section 1201(g) provides an exemption for  
13 encryption research. However, this exemption for research did not exist at first. See S. Rep. No.  
14 105-190, 1998 WL 239623 at 15-16 (1998) (as cited in Joseph Liu, Symposium: The Law and  
15 Technology of Digital Rights Management, 18 Berkeley Tech. L.J. 501 n.16 (Spring 2003)).  
16 Rather, Congress initially believed that the DMCA would rarely interfere with research and  
17 education since the research would not involve circumventing protections measures that were  
18 already in commercial use. *Id.* However, after testimony from members of the research  
19 community, Congress provided a research exemption. Yet, this exemption is of no help to  
20 Defendants because the DMCA requires that circumvention research is conducted in “good faith”  
21 and the researcher made an effort to obtain authorization from the copyright owner before  
22 engaging in the circumvention. 17 U.S.C. 1201(g)(2). Here, none of the Defendants made any  
23 such attempts.

24 Comments made after the passage of the DMCA also support the court giving the DMCA  
25 an expansive reading as required by the language in the statute itself. Senator Orrin Hatch, the co-  
26 sponsor of the DMCA, stated that the “DMCA is the most comprehensive bill that has come  
27 before the Senate regarding the Internet and the digital world in general.” Bonnie Schriefer,  
28 Comment: “Yelling Fire” and Hacking, 71 Fordham L. Rev. 2283, 2301 (April 2003). Senator

1 Hatch also went on to note that American companies were losing “\$18 to \$20 billion annually due  
2 to the international piracy of copyrighted works.” Id. Given these declarations of the DMCA’s  
3 purpose and Congress’ goal of eradicating the global epidemic of the piracy of copyrighted works,  
4 it is clear that the legislative intent supports using the DMCA to the fullest extent possible. The  
5 huge economic losses imposed and the inability of former laws to deal with the problem of digital  
6 piracy all indicate that Congress intended the DMCA to become a powerful weapon to combat the  
7 piracy of copyrighted works.

8 B. The Technological Protection Measure Used by the 5C Method of Encryption  
9 Successfully Prevents Circumvention of the Encryption by People With Ordinary  
10 Technical Skills and Computing Power.

- 11 1. 5C encryption is effective because it prevents the vast majority of the  
12 population from accessing copyrighted material and there are no readily  
13 available cost-effective alternatives.  
14

15 In order to circumvent the 5C encryption technology, specialized knowledge and  
16 tremendous computing power are required. Johnson was not able to circumvent the technology by  
17 exploiting underlying weaknesses in the technology. Expert Statement of C. Bradley Hunt ¶12.  
18 Rather, Johnson’s circumvention system allowed him to organize a vast network of computers  
19 together and implement a brute force attack on the 5C encryption. By utilizing such a system of  
20 attack, it is only a matter of time before an encryption key is successfully circumvented.  
21 However, the C5 system is still effective because for every two minutes of video there is a  
22 different encryption key. Thus, in order to effectively circumvent the system, one would have to  
23 obtain multiple encryption keys which would be a very time consuming process. This feature  
24 makes it an effective copyright protection measure. Expert Statement of C. Bradley Hunt ¶12.  
25

26 Furthermore, the current 5C encryption method is effective because there are no other  
27 readily available alternatives. First and foremost, the adoption of longer encryption methods  
28

1 would make all existing consumer devices that use this method of encryption obsolete. Expert  
2 Statement of C. Bradley Hunt ¶15. As a result, any attempt to improve an already robust system  
3 would impose a tremendous cost on the public. Furthermore, it is very costly to design protection  
4 measures to defend against professional, organized attacks, because even if the most advanced and  
5 complicated technology is used, it can still always be hacked in the future as long as certain expert  
6 hackers are intently working to circumvent it. Expert Statement of C. Bradley Hunt ¶14. Thus,  
7 what is needed is strict enforcement of the laws already on the books to prevent and discourage  
8 expert individuals from circumventing the copyright protection mechanisms.  
9

10  
11 Finally, the 5C encryption is effective because it requires a great deal of skill to circumvent  
12 the protections. An ordinary computer user with some familiarity with programming would be  
13 unable to circumvent the current 5C technology. In this case, Johnson was only able to undermine  
14 this effective encryption system by providing a complicated program for decryption that allowed  
15 users with insufficient knowledge and meager processing power to access decryption keys  
16 illegally. Expert Statement of C. Bradley Hunt ¶13. Thus, the ordinary user would be prevented  
17 from accessing the protected material. Even the more expert hackers would be unable to penetrate  
18 the defenses of this system unless they are able to link a vast network of computers and mount a  
19 sustained brute force attack.  
20

21 2. 5C encryption, in the ordinary course of its operation, requires the authority  
22 of the copyright owner to gain access to the protected work.  
23

24 Since the DMCA defines what effective means in the text of the statute, that is the most  
25 persuasive and definitive explanation for a given term. Here, a technological measure is effective  
26 if the measure, in the ordinary course of its operation, requires the authority of the copyright  
27 owner in order to gain access to the work. 17 U.S.C. 1201(a)(3)(B). 5C encryption works by  
28

1 requiring the authority of the copyright owner, provided in digital encryption, in order for the user  
2 to gain access to the work. This technological protection measure performs this function in the  
3 ordinary course of its operation. As a result, the 5C encryption is effective within the meaning of  
4 the DMCA.  
5

## 6 7 **II. The First Amendment to the United States Constitution does not Prevent** 8 **Enforcement of the DMCA.**

9 The First Amendment provides that “Congress shall make no law ... abridging the freedom  
10 of speech. U.S. Const. amend I. Case law clearly establishes that the First Amendment is not per  
11 se violated by the DMCA. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)  
12 (DMCA does not violate First Amendment); Universal City Studios, Inc. v. Reimerdes, 82 F.  
13 Supp. 2d 211 (S.D.N.Y. 2000) (same). However, the First Amendment might still be violated if  
14 the DMCA as applied to the facts of this individual case violate the Supreme Court’s First  
15 Amendment jurisprudence. However, the first step in any First Amendment analysis is whether  
16 there is any speech that is being regulated. Therefore, any potential First Amendment claim  
17 hinges on whether or not Johnson’s circumvention method is speech. Given the functions  
18 performed by Johnson’s program, there is no speech being regulated by the DMCA.

### 19 A. Johnson’s Circumvention Program is not Speech Within the Meaning of the First 20 Amendment.

21 Here, the code manufactured by Johnson does not survive the initial test of qualifying as  
22 speech. Johnson’s code might be considered speech protected by the First Amendment if it  
23 conveys some sort of information. University City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir.  
24 2001). Although the court in Corley held that the software program at issue was speech, it did so  
25 only because the DeCSS code conveyed information. Corley, 273 F.3d at 447. Here, however,  
26 the computer code designed by Johnson serves no such communicative purpose. Rather, the code  
27 serves a non-speech function of enabling the circumvention of 5C encryption technology. Unlike  
28 the code in Corley which could fairly be characterized as serving a communicative function

1 between computer programmers, Johnson’s technology is used in a mechanical and automated  
2 way. Johnson’s code allows computers to link and form a super-computer in an effort to brute  
3 force attack the encryption keys of a protected device. No communication takes place between  
4 anyone. All that the program does is allow the linking of computers in an automatic system. As  
5 such, the program designed by Johnson is not speech and is therefore not protected by the First  
6 Amendment.

7 B. Even if the First Amendment Protections Apply to Material Covered by the DMCA,  
8 Such Material Would be Commercial Speech Which Congress can Constitutionally  
9 Regulate.

- 10  
11 1. Since the government regulation is content neutral, the regulation of speech  
12 is subject to the lesser standard of intermediate scrutiny.

13 Regulations deemed content neutral are judged under the less searching standard of review  
14 known as intermediate scrutiny. Turner Broad Sys., Inc. v. FCC, 512 U.S. 622, 642-643 (1994).  
15 This lesser level of scrutiny is warranted because regulations which are unrelated to the content of  
16 speech pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue.  
17 Turner, 512 U.S. at 642. Here, the DMCA regulation is content neutral because the Government  
18 is not interested in the ways that computer programmers seek to express themselves, but is instead  
19 interesting in promoting the legitimate government interest of protecting digital property rights.  
20 Thus, the DMCA is not suppressing the content of expression but is regulating the effect the  
21 speech will have on others, namely the circumvention of technological protection measures. As a  
22 result, intermediate scrutiny is the proper standard to use when examining this regulation of  
23 speech.

24  
25  
26 Since the DMCA is content-neutral, intermediate scrutiny only requires that an “important  
27 government interest” is served and the regulation does not “burden substantially more speech than  
28 necessary to further that interest.” United States v. O’Brien, 391 U.S. 367, 377 (1968). In this

1 case, the important government interest is the protection of digital information and TPMs in  
2 addition to preventing the unauthorized copying of copyrighted works. This clearly rises to the  
3 level of important government interest. United States v. Elcom, Ltd., 203 F. Supp. 2d 1111, 1129-  
4 30 (N.D. Cal. 2002). Furthermore, the DMCA regulations do not substantially burden more  
5 speech than necessary to accomplish the goal of protecting copyrighted works. Congress choose  
6 the most direct path to combating the growing problem of piracy – target those who manufacture  
7 and distribute the tools that enable the infringement of protected materials to take place. Although  
8 Congress may have taken different means to reach the same outcome of eliminating piracy, like  
9 increasing penalties for direct infringement, these methods would not be as effective as the path  
10 Congress did choose. Elcom, 203 F. Supp. 2d at 1132.

11 Thus, the DMCA as applied to the Johnson circumvention program survives intermediate  
12 scrutiny and does not violate the protections afforded by the First Amendment.

13 2. Even if the court applies strict scrutiny to the regulation, the regulation of  
14 speech does not violate the First Amendment.

15 Even if this court decides to apply a higher strict scrutiny standard to the regulation at issue  
16 in this case, the speech still does not violate the First Amendment. If the court finds that the  
17 DMCA imposes a content-based restriction, than the regulation must be narrowly tailored to serve  
18 a compelling state interest. Perry Ed. Assn. v. Perry Local Educators’ Assn., 460 U.S. 37, 45  
19 (1983). A regulation is narrowly tailored only when “the means chosen do not ‘burden  
20 substantially more speech than is necessary to further the government’s legitimate interests.’”  
21 Turner Broadcasting Systems, Inc. v. FCC, 512 U.S. 622, 662 (1994) (citing Ward v. Rock  
22 Against Racism, 491 U.S. 781, 799 (1989)).

23  
24  
25 This stricter standard is also met by the DMCA although applying such a standard would  
26 be in sharp contrast to the case law applying intermediate scrutiny to the DMCA. First, the  
27 compelling state interest is the protection of copyrighted material. As demonstrated by the  
28 Congressional intent discussed above, the protection of copyrighted information is a high priority

1 and clearly qualifies as a compelling state interest. Secondly, the DMCA is narrowly tailored  
2 since the regulation is not overbroad at who it targets. The DMCA does not target everyone  
3 engaged in circumvention and only applies to specific acts as described in the statute.  
4 Additionally, such a burden on speech is necessary in order to accomplish the government interest  
5 in reducing copyright piracy. There are no less burdensome alternatives that would just as  
6 effectively accomplish the goal of ending piracy. As a result, the DMCA even survives strict  
7 scrutiny under the First Amendment analysis.

8  
9 **III. Vicarious Criminal Liability Need Not Apply to Sundance Law, Caltech, and Dr.**  
10 **Baltimore Because All of The Defendants Directly Violated The Digital Millennium**  
11 **Copyright Act and Caused Circumvention of Digital Management Technology.**

12 John Johnson initially created his programs for educational purposes in compliance with  
13 Professor Law's course at Caltech. The initial concept was not done for the purpose of gaining a  
14 commercial advantage or financial gain as prescribed by 17 U.S.C. § 1202(a) and was not a  
15 violation of this code.

16 Law's actions were permissible the first time he used the program to gain decryption keys  
17 of 5C technology in order to circumvent technology that controls the distribution of copyright  
18 material because his actions fell under 17 U.S.C. § 1201(d), an exception created to protect  
19 educational institutes from criminal liability for a good faith determination of whether it is  
20 possible to circumvent copyright protection technology so long as their actions are not done  
21 willfully for commercial purposes.

22 The United States does not contend that the initial use of this program falls under 17  
23 U.S.C. § 1201 because its initial use was in fact for educational purposes, but rather the  
24 subsequent distribution on the Caltech website falls under acts that are prohibited. Defendants are  
25 criminally liable because they willfully participated in creating and maintaining a computer  
26 program to circumvent a technological measure that effectively controls access to a work  
27 protected under Title 17 for commercial advantage and financial gain.

1 A. Sundance Law, John Johnson, Dr. Baltimore, and Caltech Willfully Violated 17  
2 U.S.C. § 1201 for Commercial Advantage and Financial Gain When the Class  
3 Website Enabled Internet Users to Obtain Decryption Keys to Circumvent 5C  
4 Technology and are Culpable Under 17 U.S.C. § 1204.

5 Congress created the No Electronic Theft Act of 1997 (NET) to clarify criminal copyright  
6 statutes to make it clear that willful infringement of a copyright for purposes of commercial  
7 advantage or private financial gain included the reproduction or distribution of copyrighted works  
8 by electronic means. 17 U.S.C. § 506 (a). Since the DMCA also deals with criminal copyright  
9 matters and NET was a modification to the entire Copyright Code it is logical that a violation of  
10 17 U.S.C. § 1201(a) would likewise occur if a person reproduced or distributed the keys to digital  
11 management technology through electronic means and that this would constitute a willful  
12 circumvention of digital management technology for commercial advantage or financial gain.  
13 Case law supports this extension from Copyright Law to the DMCA. If a work is entitled to  
14 protection under the Copyright Act, trafficking in a device that circumvents technological  
15 measures constitutes a clear violation of 17 U.S.C. 1201(a) of the DMCA. Lexmark Int’l, Inc. v.  
16 Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003).

17 **Willful**

18 The Supreme Court defined willful in Transworld Airlines, Inc. v. Thurston, 496 U.S. 111,  
19 at 128-129 as the person “either knew or showed reckless disregard for the matter of whether its  
20 conduct was prohibited...” Here, Sundance Law was the professor of this class website and knew  
21 that the material placed on the website was able to circumvent media technology regulated by 17  
22 U.S.C. § 1201(a). As the professor of this class, he was in charge of the material placed on the  
23 class website and his failure to remove information when he was aware of the capability of the  
24 program was at least a reckless disregard for the matter of his conduct prohibited by the 17 U.S.C.  
25 § 1201(a). When the United States government warned Law that criminal charges were pending,  
26 his subsequent refusal to remove this illicit material constituted a continuing violation and  
27 conscious disregard of the law sufficient to meet the willful standard of 17 U.S.C. § 1201(a).

1 Similarly, Dr. Baltimore as President of the university and Caltech as an institution had the  
2 ability to stop the distribution of an illegal program since the material was on a Caltech website.  
3 Caltech could have shut down the website or removed the program by not allowing it to be  
4 distributed on their network. “Providing site and facilities for known infringing activity is  
5 sufficient to establish contributory liability.” Fonovisa Inc. v. Cherry Auction, Inc., 76 F.3d 261,  
6 264 (9th Cir. 1996). Since providing the facilities rises to contributory liability in a civil context,  
7 it would stand to reason that defiance of a government request to cease criminal activity rises to  
8 the level of willful.

9 Caltech also had an integral role in the circumvention of technology by providing the  
10 resources to Caltech students to link their computers through the Caltech network. Johnson sent  
11 out an email to Caltech student in order to create a supercomputer that processes the keys used to  
12 circumvent the 5C technology. Professor Law understood that the supercomputer would require  
13 Caltech resources. After notification by the Department of Justice of this illegal activity, Dr.  
14 Baltimore and Caltech could have prevented students from using the university’s resources to  
15 circumvent the 5C technology. At the very least, Dr. Baltimore should have warned his students  
16 of the potential criminal involvement to stop the student’s active participation. Dr. Baltimore and  
17 Caltech’s refusal to comply with the Department of Justice request of removing their website  
18 along with allowing students to use their resources for criminal activity constitute a willful  
19 violation of 17 U.S.C. § 1201(a).

20 Caltech and Dr. Baltimore, as the head of the institution, had an obligation to make sure  
21 the students and employees of Caltech are not using university resources to assist in activities that  
22 are known to be criminal in nature. At the minimum, they showed a conscious disregard for the  
23 matter of which their conduct was prohibited, which is sufficient to meet the willful standard.

#### 24 **Commercial Advantage**

25 The Supreme Court has defined a commercial use as being something broader than just for  
26 monetary gain but also where “the user stands to profit from exploitation of the copyrighted  
27 material without paying the customary price.” Harper & Row Publishers Inc. v. Nation  
28 Enterprises, 471 U.S. 539, 562 (1985). Commercial use refers to monetary benefits gained

1 without paying the owner for such copyrighted material. Congress decided to use a much stricter  
2 word when it created the DMCA. Congress used the word “advantage” instead of “use.”  
3 Advantage is defined in Webster’s 3rd New International Dictionary as “the benefit or gain of any  
4 kind.” This is a stricter standard because the benefit or gain does not have to be a profit without  
5 paying the customary price, but just has to benefit the user in a commercial sense.

6 The Ninth Circuit held in A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015 (9th  
7 Cir. 2001) that “repeated and exploitive copying of copyrighted works, even if the copies are not  
8 offered for sale, may constitute a commercial use.” In Napster, an Internet service called Napster  
9 facilitated the transmission and retention of digital audio files by its users through a free software  
10 that it provided. The record companies and music publishers subsequently filed copyright  
11 infringement actions against Napster for the use of the digital files.

12 Similarly, in Worldwide Church of God v. Philadelphia Church of God, 227 F.3d 1110,  
13 1118 (9th Cir. 2000) the Ninth Circuit held that a church that copied religious texts for its  
14 members “unquestionably profit[ed]” from the unauthorized “distribution and use of [the text]  
15 without having to account to the copyright holder.” See, American Geophysical Union v. Texaco,  
16 Inc., 60 F.3d 913, 922 (2d Cir. 1994) (finding that researchers at for-profit laboratory gained  
17 indirect economic advantage by photocopying copyrighted scholarly articles); Sega Enters Ltd. v.  
18 MAPHIA, 857 F. Supp. 679, 687 (N.D. Cal.1994) (finding commercial use when individuals  
19 downloaded copies of video games “to avoid having to buy video game cartridges”).

20 In this case, Internet users gain access to Johnson’s program on the Caltech website to gain  
21 keys that enable them to circumvent 5C protocol designed to protect copyrighted material. This  
22 enables distribution of copyrighted materials in order for people to avoid having to buy the  
23 respected copyrighted materials, thus constituting a commercial use.

#### 24 **Financial Gain**

25 The definition of a financial gain for the purpose of criminal copyright actions includes  
26 trading infringing copies of a work for other items includes the “receipt, or expectation of receipt  
27 of anything of value, including the receipt of other copyrighted works.” No Electronic Theft Act  
28 of 1997 § 2(a). See also, 17 U.S.C. § 101.

1 In this case, the defendants created a program that creates keys, which is an item of value  
2 that can be traded across the Internet. These items unlock copyright protections to allow potential  
3 users to gain full access to copyrighted materials without having to pay for the materials. These  
4 keys effectively destroy the purpose behind the digital management technology and run contrary  
5 to the Congressional intent to protect copyright materials.

6 The United States further offered to drop charges in exchange for Caltech removing  
7 Johnson's website and prohibiting Professor Law from teaching his course in the future, but the  
8 defendants refused. By allowing the website to remain open to the public it no longer served as an  
9 educational purpose, but instead acted in violation of 17 U.S.C. § 1201(a), "No person shall  
10 circumvent a technological measure that effectively controls access to a work protected under this  
11 title". John Johnson, Sundance Law, Dr. Baltimore, and Caltech all willfully participated in  
12 circumventing the 5C technology by creating, maintaining, and providing the means for  
13 themselves as well as others to circumvent technology.

14 B. Professor Law, Dr. Baltimore, and Caltech can Also be Found to Willfully Violate  
15 17 U.S.C. § 1201 for Commercial Advantage and Financial Gain When They Have  
16 Actual Knowledge of Infringing Activities and They Refuse to Remove it From  
17 Their System.

18 In Napster, the court found that there is another way in which a person can be found to be a  
19 direct infringer. The court held that "if a computer system operator learns of specific infringing  
20 material available on his system and fails to purge such material from the system, the operator  
21 knows of and contributes to direct infringement." Napster, 239 F.3d at 1023.

22 Here, the defendants have direct control over their computer system. Law has supervision  
23 of his class website, while Caltech and Dr. Baltimore have control over their network and  
24 university websites, property that they in fact own. Caltech's own policies of Acceptable Use of  
25 Electronic Information Resources, February 2003, signed by Dr. Baltimore, state, "Electronic  
26 information resources are intended to be used to carry out the legitimate business of the  
27 Institute.... In addition, faculty, staff, students, and other members of the Institute community,  
28 who use the Institute's electronic information resources assume responsibility for their appropriate

1 use and agree to comply with all relevant Institute policies and all applicable local, state, and  
2 federal laws.” David Baltimore, Institute Policy on Acceptable Use of Electronic Information  
3 Resources.<sup>1</sup> (See Attached Exhibit #1).

4 This policy further states that, “Some examples of inappropriate use are ... violation of  
5 copyrights, software license agreements, patent protections and authorizations, or protections on  
6 proprietary or confidential information.” Id. The University further reserves the right to review  
7 and retain data of members of the Institution at any time without prior notification, for legitimate  
8 Institute reasons. Id. Finally, the policy makes clear that, “The use of Institution electronic  
9 information resources is a privilege, not a right, and the Institute may revoke this privilege, or  
10 decline to extend this privilege, at any time.” Id.

11 Caltech and Dr. Baltimore in their policies have provided themselves with the right to  
12 control content placed on their websites and further provide the University with the right to revoke  
13 any electronic privileges granted. Rules have been set that all students and faculty not violate  
14 local, state, and federal laws particularly mentioning that they not violate copyrights and software  
15 license agreements. Id.

16 Likewise in Napster, “if a computer system operator learns of specific infringing material  
17 available on his system and fails to purge such material from the system, the operator knows of  
18 and contributes to direct infringement.” Napster, 239 F.3d at 1023. Caltech is a computer system  
19 operator that learned of specific infringing material from the government and it refused to remove  
20 the illegal program so they should be held criminally liable for such conduct. Dr. Baltimore and  
21 Sundance Law had control over the website as well, but refused to remove the offensive material,  
22 so should likewise be found criminally liable for their actions.

23  
24 **IV. Defendants are Criminally Liable for Willfully Violating 17 U.S.C. § 1201(b)(1) for**  
25 **Trafficking in Circumvention Technology for Commercial Advantage or Financial**  
26 **Gain.**

27  
28 

---

<sup>1</sup> Available at: <http://cit.hr.caltech.edu/policies/2003/ElectronicInfo02-2003.pdf>.

1 17 U.S.C. § 1201(b)(1) prohibits any person from “offering to the public or otherwise  
2 traffic in any technology, product or service... that: has only limited commercially significant  
3 purpose or use other than to circumvent protection afforded by technological measure that  
4 effectively protects a right of a copyright...” The statutory intent behind this section shows that  
5 “Congress sought to ban all circumvention tools because most of the time those tools would be  
6 used to infringe a copyright.” United States v. Elcom, 203 F. Supp. 2d 1111, 1125 (N.D. Cal.  
7 2002). In the legislative history, Congress sought to promote electronic commerce while  
8 protecting the rights of copyright owners, particularly in the digital age where near exact copies  
9 can be made at little to no cost and distributed instantaneously worldwide. S. Rep. No. 105-190 at  
10 8 (1998), Burton Decl. Exh. P. “Most acts of circumventing a technological copyright protection  
11 measure will occur in the course of conduct which itself implicates the copyright owners rights.”  
12 Id. at 29. Congress’s intent is clear, as is the statutory language, because Congress specifically  
13 banned offering to the public, the trafficking, and the marketing of all circumvention devices.

14 Here, defendants Caltech and Dr. Baltimore knew that criminal actions were pending  
15 against Professor Law and John Johnson and they understood the potential criminal penalties  
16 against all parties because the defendants were advised by the Department of Justice to remove the  
17 illegal program from their website. By continuing to offer to the public the tools used to  
18 circumvent digital management technology, the parties willfully violated 17 U.S.C. § 1201 (b)(1).

19  
20 **V. Sundance Law, Caltech, and Dr. Baltimore are Criminally Liable for Aiding and**  
21 **Abetting the Criminal Circumvention of Digital Management Technology That is**  
22 **Used to Protect Copyright Infringement.**

23 The Copyright Act only expressly imposes liability on anyone who directly infringes  
24 copyrights but “courts have long recognized that in certain circumstances, vicarious or  
25 contributory liability will be imposed.” Fonovisa, 76 F.3d at 261. The United States Supreme  
26 Court reaffirmed this principle of copyright law in Sony Corp. of America v. Universal City  
27 Studios, Inc., 464 U.S. 417, 435 (1984) that “vicarious liability is imposed in virtually all areas of  
28 the law and the concept of contributory infringement is merely a species of the broader problem of

1 identifying circumstances in which it is just to hold one individually accountable for the  
2 accountable for the actions of another.” See, Inwood Laboratories v. Ives Laboratories, 456 U.S.  
3 844, 844-6 (1982) (vicarious and contributory infringement can occur under trademark  
4 infringement even though not explicitly mentioned in the statutes).

5 Furthermore, 18 U.S.C. § 2(a) provides that “Whoever commits an offense against the  
6 United States or aids, abets, counsels, commands, induces or procures its commission, is  
7 punishable as a principal.” The DMCA does not carve out an exception to the criminal sanctions  
8 that would apply under 18 U.S.C. §2 and a plain reading of the text suggests 17 U.S.C. §1204  
9 defines a criminal offense as violating 17 U.S.C. §1201 and 17 U.S.C. §1202. Therefore, criminal  
10 liability can be imposed against Sundance Law, Caltech and Dr. Baltimore under the theory of  
11 aiding and abetting.

12 As mentioned above, without the contribution of all of the defendants in providing the  
13 resources, the circumvention of digital management technology would not have occurred, and by  
14 knowingly refusing the government’s request to remove the criminal circumvention technology,  
15 the criminal circumvention of digital management technology would not have occurred. Since all  
16 of the defendants played a major role in aiding the commission of a circumvention of digital  
17 management technology, they should all be held accountable.

18 The defense applies tests of vicarious liability from case law that is applied in the civil  
19 infringement context. Accordingly, the government responds to these issues below.

20 The Second Circuit articulated a test for vicarious liability in Gershwin Publishing Corp. v.  
21 Columbia Artists Management, Inc., 443 F.2d 1159 (2d Cir. 1971) that applies in the civil context.  
22 In this case, the Second Circuit held that “even in the absence of an employer-employee  
23 relationship one may be vicariously liable if he has the right and the ability to supervise the  
24 infringing activity and also has a direct financial interest in such activities.” Id. at 1162.

25 A. Sundance Law, Caltech, and Dr. Baltimore had the Ability to Control and Regulate  
26 the Website With the Computer Program That Allowed Circumvention of Digital  
27 Rights Management.  
28

1 In Gershwin, the defendant lacked the contractual ability to control the direct infringer, but  
2 because of the defendant’s “pervasive participation in the formation and direction” of the direct  
3 infringers, including handling advertising and promotion, the court held that the defendants were  
4 in a position to police the direct infringers. Id. at 1163.

5 Similarly in Fonovisa, 76 F.3d at 259, the Ninth Circuit applied the two-prong Gershwin  
6 test of control and financial benefit. In Fonovisa, the Ninth Circuit held that a swap meet was  
7 liable for vicarious liability based on sales of counterfeit recordings by independent vendors at  
8 their swap meets. Id. at 263. The court also held that the control prong was met because the  
9 defendant could control the infringers through its rules and regulations, the defendant patrolled the  
10 booths to make sure all of the rules and regulations were followed, and promoted the show in  
11 which the direct infringers participated. Id.

12 In this case, as mentioned above, Sundance Law, Caltech, and Dr. Baltimore have a  
13 responsibility to ensure that the university’s electronic resources do not violate copyrights and  
14 other proprietary rights. They had the ability to control the infringing information through its  
15 rules and regulations. Unlike Gershwin, however, they had the contractual right to revoke such  
16 infringements, but they refused to invoke these rights. Furthermore, the acts of Sundance Law and  
17 Dr. Baltimore can be vicariously transferred to Caltech because they have the employer/employee  
18 relationship. All these factors contribute to the defendants ability to control the illegal website and  
19 under Fonovisa the control prong is met.

20 B. Sundance Law, Caltech, and Dr. Baltimore Gained a Financial Benefit From the  
21 Circumventing Technology.

22 In Napster, 239 F.3d at 1023, the Ninth Circuit held that a “financial benefit exists where  
23 the availability of infringing material acts as a draw for customers.” In this case, the court found  
24 there was a financial benefit because virtually all of Napster’s draw resulted from Napster’s  
25 providing access to infringing material.

26 In another Ninth Circuit case, the court held that the direct financial benefit inquiry is  
27 whether there is a causal relationship between the infringing activity and any financial benefit a  
28 defendant reaps, regardless of how substantial the benefit is in proportion to a defendant’s overall

1 profits. Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004). In this case, the court held that  
2 American Online was not held vicariously liable as an internet service provider because there was  
3 no evidence presented that American Online customers subscribed to America Online in order to  
4 get the available copyrighted materials or that they cancelled subscriptions because it was no  
5 longer available. Id.

6 While the defendants may argue that Ellison is on point, there are several distinctions that  
7 must be made. First, America Online removed the service that was infringing on copyrights. Id.  
8 Second, the court in Ellison pointed to the fact that the entire service of America Online was not to  
9 get copyrighted material and that there was no evidence of people subscribing to America Online  
10 particularly for this service. Id. Third, the lower court in Ellison found that America Online had  
11 no actual knowledge of the infringement. Id. at 1078.

12 Here, people outside of Sundance Law’s class visited the classroom website with the sole  
13 intention of gaining keys to circumvent the digital management technology in order to gain access  
14 to copyrighted materials. In this case, the defendants also have actual knowledge of the  
15 infringement activities, but refused to remove the illegal material from their own website.

16 Like in Napster, financial benefit may be shown through “enhancing the attractiveness of  
17 the venue.” Napster at 1023. Caltech and Professor Law gained prestige for the university from  
18 having a highly frequented website. This belief of an increased prestige is demonstrated by  
19 Defendant Johnson’s actions. While placing the program on the class website, he also placed his  
20 resume on the website in the hope that he may get a lucrative consulting job.

21 Another distinction to be drawn from Ellison v. Robertson is that the Ninth Circuit did not  
22 apply the definition of financial gain as found under the No Electronic Theft Act of 1997 (NET)  
23 because Ellison was a civil suit. NET was created to clarify criminal copyright infringements.

24 In this case, there are criminal infringement suits so the NET definition does apply. This  
25 definition states that a financial gain is a “receipt, or expectation of receipt, of anything of value,  
26 including the receipt of other copyrighted works.” As stated above, the keys are an expectation of  
27 receipt of something of value, therefore Sundance Law, Caltech, and Dr. Baltimore gained a  
28 financial benefit from the circumventing technology.

1 It is clear that Sundance Law, Dr. Baltimore, and Caltech had the necessary control and  
2 gained a financial benefit from this circumventing technology. The defendants made a calculated  
3 decision to create, maintain, and distribute this circumventing technology to the public and should  
4 therefore be held accountable for their decision because they had the control to stop it from  
5 happening. Just like the captain of a pirate ship is responsible for the actions of his crew, the  
6 Defendants should be held accountable for the actions of those that they had the necessary control  
7 over in addition to gaining a financial benefit for themselves.

8  
9 **CONCLUSION**

10 For the reasons discussed above, the Defendants motion to dismiss the indictment should  
11 not be granted. The 5C technology was effective within the meaning of the DMCA, there is no  
12 First Amendment issue protecting the Defendants conduct, and Defendants are vicariously liable.  
13 This court should strike a blow against the new technological pirates and enforce the provisions of  
14 the DMCA as the plain language and Congressional intent demand. Defendants' motion to  
15 dismiss should be denied.

16 Respectfully submitted,

17  
18  
19 \_\_\_\_\_  
20 John T. Egley  
21 Michael Matoba  
22 Iram Parveen Bilal  
23 Meng-Meng Fu  
24 UNITED STATES ATTORNEYS  
25 LOYOTECH DIVISION

26 Arif Alikhan  
27 Jim Spertus  
28 UNITED STATES ATTORNEY'S OFFICE

Attorneys for the Prosecution