

No. 06-000

IN THE

Supreme Court of the United States of America

DANIEL BALTIMORE, ET AL, PETITIONERS

V.

THE UNITED STATES OF AMERICA, RESPONDENT

**On Writ of Certiorari to the
United States District Court for the Western District of California**

BRIEF FOR THE UNITED STATES OF AMERICA

**NEDIM HALICIOGLU
LOYOLA LAW SCHOOL
919 Albany Street
Los Angeles, California 90015-1211
(213) 736-1000**

**FELICIA KATZ
CALIFORNIA INSTITUTE OF TECHNOLOGY
1200 East California Boulevard
Pasadena, California 91125
(626) 395-6811**

**JAMES W. SPERTUS
LAW OFFICES OF JAMES W. SPERTUS
149 S. Barrington Ave., #815
Los Angeles, California 90049
(310) 476-6570**

QUESTIONS PRESENTED

1. What is the standard for determining whether a Digital Transmission Content Protection technology (DTCP) *effectively* controls access to protected works, and was that standard properly applied by the District Court in upholding criminal charges against defendants under the Digital Millennium Copyright Act (DMCA), 17 U.S.C. §1201(a)(1)(A) for allegedly circumventing the ATSC “broadcast flag”?
2. Should defendants’ indictment be dismissed on the ground that the Federal Communications Commission was without statutory authority (cf. *Am. Library Ass’n v. FCC*, 406 F.3d 689 (DC Cir. 2005)) to regulate demodulation devices by requiring recognition of the broadcast flag?

**PARTIES TO THE CASE AND
RULE 29.6 STATEMENT**

The Petitioners are Sundance Law, Daniel Baltimore and John Johnson. The Respondent is the Federal Communications Commission. Neither party is publicly traded.

TABLE OF CONTENTS

	<u>Page</u>
QUESTIONS PRESENTED	1
PARTIES TO THE CASE	2
TABLE OF CONTENTS	3
TABLE OF AUTHORITIES	4
OPINION BELOW	7
JURISDICTION	7
STATEMENT OF FACTS	7
SUMMARY OF ARGUMENT	9
ARGUMENT	10
I. 5C ENCRYPTION IS EFFECTIVE WITHIN THE MEANING OF THE DMCA	10
A. 5C Encryption is the Most Economically Efficient Means of Controlling Access to Protected Material	10
B. 5C Encryption Successfully Prevents Circumvention by the Majority of Potential Copyright Infringers	11
C. 5C Encryption is a Sufficiently Effective Method of Encryption Because it Successfully Hinders Circumvention by People with Ordinary Technical Skills and Computing Power	11
D. No Cost-Effective Alternatives to 5C Encryption Technology are Currently Available	12
II. BOTH CONGRESSIONAL MANDATE AND JUDICIAL RULINGS PROVIDE THE FCC WITH THE PROPER AUTHORITY TO REGULATE DEMODULATING DEVICES WITH REGARD TO THE BROADCAST FLAG.....	13
A. The FCC’s general jurisdiction is broad enough to cover regulation of demodulating devices	13
B. The FCC has specific authority to prescribe regulations to protect public interests like copyright protection	15
C. The FCC has jurisdiction to ensure that all receiving devices adequately receive all frequencies allocated by the Commission, specifically with regard to Digital Television	15
D. The FCC has specific authority to regulate various devices that control content after broadcasts are received	16
III. ALTHOUGH FIRST AMENDMENT ISSUES ARE OUTSIDE THE SCOPE OF CERTIORARI, THE DMCA TARGETS ONLY NON-SPEECH ELEMENTS OF COMPUTER CODE AND, THEREFORE, FAIR USE CONCERNS ARE NOT IMPLICATED BY THE STATUTE.....	17
CONCLUSION	18

TABLE OF AUTHORITIES

<u>CASES</u>	<u>Page</u>
<i>321 Studios v. MGM Studios, Inc.</i> , 307 F. Supp. 2d 1085 (N.D. CA 2004).....	17
<i>AM. Library Ass’n v. FCC</i> , 406 F.3d 689 (DC Cir. 2005).....	14, 16
<i>Autoskill, Inc. v. Nat’l Educ. Support Sys.</i> , 994 F.2d 1476 (10 th Cir. 1993).....	16
<i>CBS v. FCC</i> , 629 F.2d 1 (DC Cir. 1980).....	17
<i>Chevron, U.S.A., Inc. v. NRDS, Inc.</i> , 467 U.S. 837 (1984).....	13-15
<i>Consumer Elecs. Ass’n v. FCC</i> , 358 U.S. App D.C. 180 (DC Cir. 2003).....	15-16
<i>E.I. Du Pont de Nemours & Co. v. Christopher</i> , 431 F.2d 1012 (5 th Cir. 1970).....	10
<i>FCC v. Midwest Video Corp.</i> , 440 U.S. 689 (1979).....	17
<i>FCC v. Wncn Listeners Guild</i> , 450 U.S. 582 (1981).....	15
<i>Klitzner Industries, Inc. v. H.K. James & Co.</i> , 535 F. Supp. 1249 (E.D. PA 1982).....	15
<i>MGM Studios Inc. v. Grokster, Ltd.</i> , 125 S. Ct. 2764 (2005).....	15
<i>National Broadcasting Co. v. U.S.</i> , 319 U.S. 190 (1943).....	15
<i>Pension Benefit Guar. Corp v. LTV Corp.</i> , 496 U.S. 633 (1990).....	17
<i>RIAA v. Verizon</i> , 257 F. Supp. 2d 244 (DC Cir. 2003).....	17
<i>Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.</i> , 925 F.2d 174 (7 th Cir 1991).....	12
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2 nd Cir. 2001).....	17
<i>Universal Studios v. Reimerdes</i> , 111 F. Supp 2d 294 (S.D. NY 2001).....	17
<i>US v. Elcom Ltd.</i> , 203 F. Supp 2d 1111 (N.D. CA 2002).....	17
<i>U.S. v. Mead Corp.</i> , 533 U.S. 218 (2001).....	14
<i>U.S. v. Southwestern Cable Co.</i> , 392 U.S. 157 (1968).....	14, 17
<i>Yee v. City of Excondido</i> , 503 U.S. 519 (1992).....	17

<u>STATUTES, CONSTITUTIONS and AGENCY MATERIAL</u>	<u>Page</u>
17 U.S.C. §1201 (a)(3)(B).....	8
47 USCS §151.....	13
47 USCS §153(52).....	14
47 USCS §303(s).....	15
47 USCS §303(u).....	16
47 USCS §303(x).....	16
47 USC §309(j)(14)(A).....	16
47 USCS §336 (b)(4), (5).....	13, 15
<i>In the Matter of Digital Broadcast Copy Protection</i> , 17 FCCR 16027.....	15-17
<i>United States Constitution</i> , Article 1, Section 8.....	9
 <u>MISCELLANEOUS</u>	
<i>2004 Piracy Fact Sheets: US Overview</i> , Motion Picture Association of America – available at http://www.mpaa.org/USPiracyFactSheet.pdf	9
<i>Business Objects Tightens Security, Reignites Encryption Debate</i> , Computer Business Review (2005).....	12
<i>Copyright Issues in Digital Media</i> , US Copyright Office (2004) - available at http://www.cbo.gov/showdoc.cfm?index=5738&sequence=1	9
<i>CS-Cipher Challenge</i> , Distributed.net (2000) – available at http://www.distributed.net/projects.php	11
<i>Digital Transmission Content Protection</i> , Intel (1999) – available at http://www.dtcp.com/data/dtcp_tut.pdf	11
<i>Extracting a 3DES Key from an IBM 4758</i> , Richard Clayton (2001) – available at http://www.cl.cam.ac.uk/~rnc1/descrack	12
<i>Nimmer on Copyright</i> §1.03	15

	<u>Page</u>
<i>NIST Says DES Encryption “inadequate”</i> , IDG News Service (2004) – available at http://www.infoworld.com/article/04/07/29/HNdesinadequate_1.html	12
<i>Second Annual BSA and IDC Global Piracy Study</i> , Business Software Alliance (2005) – available at http://www.bsa.org/globalstudy	10
<i>What is the V-Chip</i> , Family Safe Media – available at http://www.familysafemedia.com/v-chip.html	16

OPINION BELOW

The opinions below can be found at 406 F.3d 689, and at 25 Loy. L.A. Ent. L. Rev. 55 (2004) – available at <http://techlaw.lls.edu/events/atc2004/opinion.pdf>.

JURISDICTION

Jurisdiction in the Court of Appeals for the 12th Circuit was proper under 28 U.S.C. §1292(b), after certification by the District Court that the Order appealed from and involved a controlling question of law as to which there was substantial ground for difference of opinion. Prior to hearing by that court, this Court granted certiorari pursuant to 28 U.S.C. §1254 because of the importance of the issue and because of an apparent conflict among the circuits.

STATEMENT OF FACTS

In the Fall of 2003, professor Sundance Law of the Calculating Institute of Technology (Caltech) taught a course on Digital Protection. During the course, Law, divided up the class into two teams. One of these teams was given the task of devising a technological protection measure (a TPM), while the other team had the task of hacking or bypassing the TPM's. For his assignment, student Dimitry Skylore (Skylore) developed a TPM that protected both access to and use of digital content. Skylore's TPM encrypted content and also contained copy control information (CCI) which set permissions for whether or not the content could be copied, and if so, how many times it could be copied.

Johnson was the student assigned to hack Skylore's TPM. His strategy was to decrypt the CCI and set the permissions to allow for an infinite number of copies and distribution. Then, after the content was decrypted he would be able to freely copy and distribute it. Because Skylore used 56-bit encryption – significant computing power was needed to break it. In order to hack Skylore's encryption, Johnson devised a "brute force" method of trial and error. In order to do this, Johnson employed the use of many of individual computers over the internet working together. Using this distributed computing method, volunteers would let their computers work on separate pieces of decrypting Skylore's DRM. Within 24 hours Johnson's method cracked Skylore's DRM and Johnson posted the results on his web site.

Subsequently, Law realized that Skylore's TPM was similar to the "5C" Broadcast Flag technology being developed by the entertainment industry in conjunction with consumer electronics companies. Accordingly, Law posted a short 5C encrypted video on Johnson's web site, and within a day the correct decryption key was found, and Law was able to copy a clear version of the video. Word traveled fast that Johnson's web site could be used to decrypt protected media.

Following this, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA) and Intel (a co-inventor of the 5C technology) persuaded the US Department of Justice (DOJ) to bring criminal charges against Johnson, Law,

Caltech and its president, Daniel Baltimore. All defendants moved to dismiss the indictment on various grounds. District Judge Ronald Lew granted Caltech's motion to dismiss, but denied all other defendants. The decision is appealed here.

In the proceedings below, the District Court granted defendant Caltech's motion to dismiss the indictment charging it with a violation of the Digital Millennium Copyright Act (DMCA) on the ground that the DMCA plainly exempted educational institutions from prosecution under the DMCA. However, the District Court denied the motion to dismiss the indictment against John Johnson (Johnson), Sundance Law (Law), and Baltimore on the ground that the indictment properly alleged each of the elements required to state an offense under the DMCA. Specifically, the District Court found that the technology at issue was effective within the meaning of the DMCA. Judge Lew's opinion, p 103. Further, the District Court also found that the defendants acted willfully and for purposes of commercial advantage or private financial gain. Finally, the District Court also found that the DMCA did not violate the defendants' First Amendment Rights. *Id* at 104.

Although the District Court did not reach the issue of whether the indictment should be dismissed on the ground that the Federal Communications Commission (FCC) was without statutory authority to regulate demodulating devices by requiring recognition of the broadcast flag, the District Court did reach the issue regarding the effectiveness of the Broadcast Flag as a content protection measure. The District Court recognized that to be effective, the technological measure need not make circumvention impossible. *Id* at 103. Citing the statutory definition of effective, the District Court ruled that the technological measure, "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work," then it is effective. 17 U.S.C. §1201 (a)(3)(B).

The District Court recognized that the statute does not specify the quantity or quality of information, processes, or treatments required to be effective. Consequently, the District Court ruled that even the application of minimal information, processes, or treatments may be considered "effective" under the statute. Judge Lew's opinion, p 104. The District Court then went on to find that the DTCP technology at issue in this case required much more than the application of minimal information, process, or treatments since, in order to circumvent the technological measures, a person would need: (1) the technical knowledge and skill to access and use a distributed computing system; (2) the patience to repeatedly subject two minute clips of video to the decryption system and then wait almost a day to obtain each key; and (3) the additional technical ability to splice these clips back together to form the full work. *Ibid*.

Applying this standard to the facts of this case, the District court found that the DTCP encryption prevented access to all except a few skilled people that would have to work for weeks to decrypt a single motion picture on DVD, and that this effort met the statutory requirement that, in the ordinary course of its operation, the work cannot be accessed without applying some information, process, or treatment supplied by the copyright owner. The District Court expressly found that extraordinary efforts would be required to circumvent the DTCP technology, and that the DTCP technology was therefore "effective" within the meaning of the DMCA.

SUMMARY OF ARGUMENT

According to the Business Software Alliance, worldwide losses due to piracy of software in 2004 were an estimated 32 billion dollars, with rates of piracy approaching 90% in several countries. *Second Annual BSA and IDC Global Piracy Study*, Business Software Alliance, p. 9 (2005) <http://www.bsa.org/globalstudy>. An additional 3.5 billion dollars are being lost annually due to piracy of movies in the United States alone. *2004 Piracy Fact Sheets: US Overview*, Motion Picture Association of America, p.1 <http://www.mpa.org/USPiracyFactSheet.pdf>. In the face of such drastic losses, efficient protection of copyrighted material must be implemented. However, the balance between what portion of that protection should be allocated to the implementation of more secure technological measures, and what portion should be allocated to litigation remains in question. We posit that the current standard 56 bit encryption represents the most economically efficient technological measure, when combined with legal protection.

Copyrights originated in England in 1556, shortly after the printing press was introduced to the public, an example of law following in the footsteps of technology. In the United States, the first federal copyright laws were laid down in Copyright Act of 1790, after the Constitution granted the federal government power to create both patents and copyrights. This act gave protection to authors for a period of time, and subsequent amendments broadened the scope of copyright protection to encompass the multitude of new media that arose. The intention of this clause was to “promote the Progress of Science and useful Arts,” in order to both incentivize creativity by conferring a reward upon the author, and to augment the public benefit from such works. *United States Constitution, Article 1, Section 8*, ratified 1788. As stated by Justice Stewart when describing the purpose of the Copyright Act, “The immediate effect of our copyright law is to secure a fair return to an ‘author’s’ creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good.” When deciding whether a technology designed to protect copyrighted material is effective, one must take into account the underlying purpose of copyrights, which is essentially an economic efficiency balance between the need to provide incentive for creative works and the need to give the public access to those works in order for their benefit to be as widely spread as possible. According to the US Copyright Office, the goal is economic efficiency, in which a balance is struck between the rights of copyright holders and consumers that maximizes net wealth. *Copyright Issues in Digital Media*, US Copyright Office, p. 1 (2004) <http://www.cbo.gov/showdoc.cfm?index=5738&sequence=1>.

One of the main goals of the US Copyright Office is to contribute to congressional deliberations on how copyright might be adapted to new technologies while maintaining protection and incentives to create. The DMCA was enacted with these intentions, and thus when interpreting the meaning of the word “effective” in the context of the DMCA, an economic definition best exemplifies the intentions of the writers of the DMCA and the broader intentions of copyright protection. The interpretation of “effective” then describes a protection method which is more economically efficient than its counterparts while still providing the service that it was meant to provide.

ARGUMENT

I. 5C ENCRYPTION IS EFFECTIVE WITHIN THE MEANING OF THE DMCA

The District court found that the DTCP encryption prevented access to all except a few skilled people that would have to work for weeks to decrypt a single motion picture on DVD, and that this effort met the statutory requirement that, in the ordinary course of its operation, the work cannot be accessed without applying some information, process, or treatment supplied by the copyright owner. The District Court expressly found that extraordinary efforts would be required to decode the DTCP technology, and that the DTCP technology was therefore “effective” within the meaning of the DMCA. Public policy supports this ruling because it provides the most economically efficient definition of “effectiveness.”

A. **5C Encryption is the Most Economically Efficient Means of Controlling Access to Protected Material**

A combination of technological protection (the burden of which falls upon the copyright holder) and legal protection (the burden of which falls upon the government, and is indirectly absorbed by the consumer) is the most economically efficient method of copyright protection. In this case, the optimal and most robust possible technological protection is neither necessary nor advantageous, because legal measures to protect copyrighted materials are able to pick up where the technological protection drops off in efficacy at a lesser cost. See, e.g., E. I. duPont deNemours & Co. v. Rolfe Christopher et al, 431 F.2d 1012 (5th Cir. 1970), *cert. denied*, 400 U.S. 1024 (1971). DuPont involved the protection of trade secrets, but the case is highly relevant here. In DuPont, the defendants were accused of improperly acquiring trade secret information by flying an airplane over a partially completed, novel methanol plant and taking photographs. Although the plant was surrounded by a large wall, there was no roof protecting its inner workings from observers in the air. The DuPont court ruled that constructing a roof would have imposed an enormous expense on the owner, and that the wall was a sufficient precaution to maintain secrecy. “[A]n impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts.” The DuPont court ruled that the defendants had obtained the information by “improper means.”

In the case at bar, a brute-force attack such as that utilized by Johnson in acquiring the encryption key to the 5C DTCP was the copyright analog of “improper means.” Our argument rests on the tenet that the 5C DTCP 56 bit encryption is *not* an “impenetrable fortress,” and is neither completely secure nor the most robust technology available to protect digital material from copyright infringement. However, it *is* effective as properly defined by the District Court’s interpretation of the DMCA, because, it is capable of preventing all but the most skilled and inventive people from decoding encrypted media. Furthermore, it is the most economically efficient way of providing technological protection. Thus, as the District Court correctly ruled, the government has sufficiently alleged in its indictment that John Johnson, by circumventing the DTCP technology, has violated the DMCA.

B. 5C Encryption Successfully Prevents Circumvention by the Majority of Potential Copyright Infringers

5C DTCP technology was designed to protect material that was being streamed through the internet, where a continuous data flow allows viewing of the encrypted material before the entire file is completely downloaded. The specific requirements of such technology, as defined by Intel (one of the 5C companies) are as follows: (1) Authentication and Key Exchange (a unique secret key and certificate must be issued by a Digital Transmission Licensing Administrator, DTLA); (2) Copy Control Information (CCI, which determines the number of allowable copies that can be made and under what conditions); (3) Encryption (in this case a 56 bit key length); (4) Renewability (certificate can be revoked or renewed, as defined in the license agreement); (5) Licensable (e.g. patentable); (6) Robust implementation (compatible with electronic devices). *Digital Transmission Content Protection*, Intel (1999) <http://www.dtcp.com/data/dtcp/tut.pdf>.

Intel went on to describe the various types of people most likely to participate in copyright infringement: (1) Casual copier (occasionally downloads digital media); (2) Hobbyist (downloads a published circumvention of existing protective technology in order to facilitate personal downloading of encrypted media); (3) Hacker (creates circumventive programs and distributes them); (4) Small-scale pirate (in possession of circumventive technology and a store of decoded files); (5) Professional pirate (well-funded and knowledgeable).

The vast majority of copyright infringers fall under the first two categories, and those are the people most likely to be hindered by the 5C DTCP technology. As long as these ordinary users are unable to individually create programs to undermine the DRM in place, the encryption should be deemed effective. The remaining categories of copyright infringers possess technical skill and both the monetary and computing resources to mount a successful attack on technological protective devices, and the DMCA does not require that such devices inhibit attacks from these types of infringers in order to be considered “effective,” as properly defined by the District Court.

C. 5C Encryption is a Sufficiently Effective Method of Encryption Because it Successfully Hinders Circumvention by People with Ordinary Technical Skills and Computing Power

In the year 2000, in a contest sponsored by Distributed.net using a brute-force attack that took advantage of distributed computing power, the 56 bit DES (Digital Encryption Standard) was hacked in 62 days (having searched the majority of the keyspace), with a total of 38,107 participants. *CS-Cipher Challenge*, Distributed.net (2000) <http://www.distributed.net/projects.php>. Six years later, Johnson was able to hack a similar encryption system in one day using a similar technique. However, the key discovered by Johnson would only be useful for decoding two minutes of media. In order to obtain a full-length movie, approximately 120 minutes long, the program would have to run for almost two months. This would be prohibitive to video streaming, indicating that even with the massive amount of computing power utilized by Johnson, the main purpose of the DTCP technology was still upheld, and the encryption was still effective.

Prosecution expert C. Bradley Hunt testified that the secrecy of the encryption keys was undermined by the fact that millions of copies of the keys were being distributed to end-users. Because the keys were no longer secret, the technology was thus rendered ineffective. He stated that “the attack was possible because the DRM developers caused the relevant keys and other information to be published inside every single DVD player.” However, the necessity of licensing keys to end-users for the device to function precludes any accusation of lack of proper secrecy measures. See, e.g. *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*, 925 F.2d 174 (7th Cir 1991). Rockwell, which involved the protection of trade secrets but is relevant here as well, establishes that the distribution of secret information to end-users and vendors necessary for the normal functioning of the product does not constitute inadequate precaution in maintaining secrecy, because “extravagant, productivity-impairing measures to maintain secrecy” hinder the beneficial gains from the product and are economically inefficient. Regarding DRMs, all licensees of 5C DTCP technology are required to sign a disclosure agreement preventing them from sharing the keys, placing the burden of secrecy on the end-user.

D. No Cost-Effective Alternatives to 5C Encryption Technology are Currently Available

128 bit encryption technology is the strongest readily-available DRM on the market (256 bit encryption exists, but is not available for widespread use). This technology is 4.7 sextillion times more secure than 56 bit encryption and has been deemed “unbreakable.” There are no current reports of 128 bit encryptions having been hacked, but there are projects working on the task at present. However, in 2001, Richard Clayton of the University of Cambridge in London managed to crack a 168 bit equivalent triple DES encryption system in two days using brute-force hardware costing less than \$1000. *Extracting a 3DES Key from and IBM 4758*, Richard Clayton (2001) <http://www.cl.cam.ac.uk/~rnc1/descrack>. Increases in computing power according to Moore’s Law in the next decade will most likely bring about programs with the ability to compromise 128 bit technology as well.

In 2004, the National Institute of Standards and Technology (NIST) publicly announced that the 56 bit DES was no longer secure enough to protect government information, and that all files were to be subsequently protected by an Advanced Encryption Standard (AES) consisting of a 128 bit encryption. *NIST Says DES Encryption ‘inedequate’*, IDG News Service (2004) http://www.infoworld.com/article/04/07/29/HNdesinadequate_1.html. This technology has also been adopted for credit card transactions, bank records, and other highly valued information. However, the potential cost incurred if governmental information regarding national security were to be decoded is vastly higher than the loss of profits to companies producing digital media, and thus warrants the use of more expensive technological protection. DRMs based on 128 bit encryption are costly in several ways. The direct cost of a software package to implement 128 bit technology is quite high. Manufacturers of DRMs such as Cognos are beginning to sell 128 bit encryption technology as an upgrade to their standard 56 bit encryption package, at a cost of around \$7000 per device, according to a Cognos spokesperson. *Business Objects tightens security, reignites encryption debate*, Computer Business Review (2005) <http://www.cbronline.com>. And while several businesses, such as Business Objects, are beginning to implement 128 bit technology as a standard feature of their protective software,

their market is composed mainly of users and vendors of high-end devices that transmit valuable and sensitive financial information.

The direct cost of the DRM is not the only cost that would result from a total turnover from 56 bit to 128 bit technology. Almost all widely used electronic devices are compatible with 56 bit encryption DRMs but not with 128 bit encryption technology, and a massive overhaul of these devices would be required to implement more secure protection. According to the president of Public Knowledge (a technological think tank), “Current versions of TiVos and other recording devices, iPods and other MP3 players, cell phones, and PS2 portable Playstations would not work,...rendering them obsolete.” Replacing the old technology would result in a high cost to the consumers of these products. In addition, the expense of implementing this new and expensive DRM would prevent new companies from entering the market due to the prohibitive cost.

Progress in technology is able not only to produce stronger encryption power, but also more capable methods of hacking these encryptions. A costly arms race between hackers and copyright holders is not an economically efficient solution to this problem. Rather, inexpensive and already widely-implemented DRM technology such as the 5C DTCP 56 bit encryption, which is capable of preventing the vast majority of potential copyright infringers from gaining access to encrypted media, is sufficient as a technological means of protection. The cost of moving the remaining necessary protection from the technological realm to the legal realm is less than the cost of attempting to keep up with hackers by implementing stronger and more secure technological measures. Implementing 128 bit technology is not cost-effective, and 56 bit encryption is sufficiently effective under the terms of the DMCA, as properly defined by the District Court.

II BOTH CONGRESSIONAL MANDATE AND JUDICIAL RULINGS PROVIDE THE FCC WITH THE PROPER AUTHORITY TO REGULATE DEMODULATING DEVICES WITH REGARD TO THE BROADCAST FLAG

A. The FCC’s general jurisdiction is broad enough to cover regulation of demodulating devices.

Congress vested in the FCC the responsibility of regulating “communication by wire and radio...for the purpose of securing a more effective execution...by centralizing authority...” 47 USCS §151. The FCC’s power has grown through Congressional mandate since its inception. In 1996, Congress further expanded the FCC’s power, declaring that the FCC should “(4) adopt such technical and other requirements as may be necessary or appropriate to assure the quality of the signal used to provide advanced television services...and (5) prescribe such other regulations as may be necessary for the protection of the public interest, convenience, and necessity.” 47 USCS §336 (b)(4), (5).

In *Chevron, U.S.A., Inc. v. NRDC, Inc.*, this Court established that review of “an agency’s construction of the statute which it administers...” is a two step process. 467 U.S. 837 at 842 (1984). “First, always is the question whether Congress has directly spoken to the precise question at issue.” *Id.*, at 842-843. Step two is only reached if “the court determines Congress

has not directly addressed the precise question at issue...” *Id at 843*. If this is the case, “the court does not simply impose its own construction on the statute, [but rather], if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency’s answer is based on a permissible construction of the statute.” *Ibid*.

Later, this Court held that “administrative implementation of a particular statutory provision qualifies for *Chevron* deference where it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, and that the agency interpretation claiming deference was promulgated in the exercise of that authority.” *US v. Mead Corp.*, 533 U.S. 218 (2001) at 226-227. Congress has constantly been indicating that the FCC’s authority be quite vast by continuing to expand the definition of “communication by wire and radio”. Congress has specifically designated that the “term ‘wire communication’ or ‘communication by wire’ means the transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) **incidental to such transmission.**” 47 USCS §153(52), emphasis added.

The court in *Am. Library Ass’n v. FCC* drew an inexplicable line at the point which they determined a transmission had completed and stated that the FCC’s jurisdiction ended at that exact point. 406 F.3d 689 (DC Cir. 2005) at 703. There is no such imaginary wall at the point at which an initial transmission is completed. For instance, in *US v. Southwestern Cable Co.*, the court found that the FCC had jurisdiction to regulate Community Antenna Television (CATV) under 47 USCS §153(52). 392 U.S. 157 (1968) at 168 (referring to 47 USC §§ 153 (a) & (b) – now 47 USCS §153(52)). The CATV systems in question involved large antennas that were set up in urban areas that subsequently sent the received signals via cable lines to rural areas. Thus, the court held that the FCC’s jurisdiction did **not** end when the initial transmission was received by the community antenna, but rather extended to cover the forwarding of the signal to the rural areas. The court explicitly stated that the “very general terms [of 47 USCS §153(52)] amply suffice to reach the [CATV organizations] activities.” *Id*. The CATV systems at issue in *US v. Southwestern Cable Co.* would “receive television broadcast signals, amplify them, transmit them by cable or microwave, and distribute them...” *Id at 157*. Clearly, the FCC’s jurisdiction was not cut off after the initial reception of the television broadcast signals.

In the case at hand, it is clear that the FCC’s regulation of demodulator products is factually parallel with the example of CATV. Here, the FCC is regulating demodulator devices that receive a broadcast signal and send the signal to a television monitor or other household media device much like how in the CATV scenario, the community antennas would receive broadcast signals and send them to rural communities. Because the demodulator devices in question are incidental to the transmission of communication by wire and radio, they fall under the FCC’s regulatory authority. 47 USCS §153(52). This is noted in the flag order, where the drafters state that there is a “fuller meaning to the concept of ‘communication’ so as to include all ‘instrumentalities, facilities, apparatus and services’ that may be ‘incidental’ to the literal transmission, but which are a part of an overall circuit of messages that are sent and received.” 18 FCC Rcd 23550. “In the context of the developing problems to which it was directed, the

[Communications] Act gave the [FCC] not niggardly, but expansive powers.” *National Broadcasting Co. v. US*, 319 U.S. 190 (1943) at 219.

B. The FCC has specific authority to prescribe regulations to protect public interests like copyright protection

As a general principle, “the public interest is in the interest of upholding copyright protections.” *Autoskill, Inc v. Nat’l Educ. Support Sys.*, 994 F.2d 1476 (10th Cir. 1993) at 1499. Further, “it is virtually axiomatic that the public interest can only be served by upholding copyright protections...” *Klitzner Industries, Inc. v. H.K. James & Co.*, 535 F. Supp. 1249 (E.D. PA 1982) at 1259-1260. In the digital age, copyright protection is of a heightened concern. “[Digital] distribution of copyrighted material threatens copyright holders as never before, because every copy is identical to the original, copying is easy...” *MGM Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764 (2005) at 2275. Nimmer addresses this point by stating that “the authorization to grant to individual authors the limited monopoly of copyright is predicated upon the dual premises that the public benefits from the creative activities of authors, and that the copyright monopoly is a necessary condition to the full realization of such creative activities.” Nimmer on Copyright §1.03.

These policy concerns were addressed in the FCC’s Notice of Proposed Rule Making (NPRM) for the broadcast flag. The commission noted that “[digital] copy protection...unlike its analog counterpart, is susceptible to piracy because an unlimited number of high quality copies can be made and distributed in violation of copyright laws.” *In the Matter of Digital Broadcast Copy Protection*, 17 FCCR 16027.

The FCC has specifically been delegated the duty to “prescribe...regulations as may be necessary for the protection of the public interest, convenience, and necessity.” 47 USCS §336 (b)(5). The FCC’s “judgment regarding how the public interest is best served is entitled to substantial judicial deference.” *FCC v. Wncn Listeners Guild*, 450 U.S. 582 (1981) at 596. Further, the “Court has characterized the public-interest standard of the Act as ‘a supple instrument for the exercise of discretion by the expert body which Congress has charged to carry out its legislative policy.’” *Id.* at 593. The protection of valuable copyrights is clearly in the public’s interest, the FCC as such has the authority to mandate such regulations as the broadcast flag in question.

C. The FCC has jurisdiction to ensure that all receiving devices adequately receive all frequencies allocated by the Commission, specifically with regard to Digital Television.

Under 47 USCS 303(s), the FCC was given the “authority to require that apparatus designed to receive television pictures broadcast simultaneously with sound be capable of adequately receiving all frequencies allocated...” 47 USCS 303(s). In *Consumer Elecs. Ass’n v. FCC*, the DC circuit found that under this statute, the FCC had the authority to mandate that all receivers be equipped with a tuner capable of receiving and decoding digital television (DTV) signals. 358 US App. D.C. 180 (DC Cir 2003). The court in *Consumer Elecs. Ass’n* reached this conclusion through the second step of the aforementioned *Chevron* analysis. In doing so, the

court declared that for statutory interpretation purposes, “the Supreme court has consistently instructed that statutes written in broad, sweeping language...be given broad, sweeping application.” *Id* at 298.

This conclusion would in turn lead to the conclusion that the FCC has the authority to mandate that all receivers be able to adequately receive the broadcast flag signal. In the case of the broadcast flag, in order for it to function adequately, the receiver must follow the permissions encoded in the flag signal.

Further, Congress has mandated a nationwide change over to DTV as the new standard for broadcast television. 47 USC §309(j)(14)(A). The broadcast flag is an important part of this implementation plan. The DC circuit considered this factor and indicated that the “FCC found that a logjam was blocking the development of DTV: broadcasters are unwilling to provide more DTV programming because most viewers do not own DTV equipment, and the lack of attractive DTV programming makes consumers reluctant to invest more in DTV equipment...” *Consumer Elecs. Ass’n* at 300. Addressing the same concern, the FCC noted in the NPRM for the broadcast flag, that the “ongoing [DTV] transition poses many unique logistical and technological challenges. The current lack of digital broadcast protection may be a key impediment to the transition’s progress.” 17 FCCR 16027. The broadcast flag is clearly in furtherance of the Congressionally mandated goal of setting DTV as the standard for the future.

D. The FCC has specific authority to regulate various devices that control content after broadcasts are received.

In its decision in *Am. Library Ass’n*, the DC circuit stated that they could “find nothing in the statute, its legislative history, the applicable case law, or agency practice indicating that Congress meant to provide the sweeping authority the FCC now claims over receiver apparatus.” 365 U.S. App DC at 704. However, Congress has mandated that the FCC regulate receiver apparatus with regard to a number of different policies.

For instance, the FCC has been delegated the authority to regulate and require that receivers “designed to receive television pictures broadcast simultaneously with sound be equipped with built-in decoder circuitry designed to display closed-captioned television transmissions...” 47 USCS §303(u). Further, the FCC also can require that television broadcast receivers be equipped with a feature designed to enable viewers to block display of all programs with a common rating...” 47 USCS §303(x). This is the legislation that paved the way for the so-called “V-Chip” which parents could use to limit their children’s access to violent or sexual content. The V-Chip works in a remarkably similar manner as the broadcast flag. “The V-Chip intercepts a ratings code transmitted by broadcasters or video,” much like the decoders in regard to the broadcast flag receive a set of permissions transmitted along with the content. *What is the V-Chip*, Family Safe Media <http://www.familysafemedia.com/v-chip.html>. The V-Chip “then interprets the code and transmits a signal to [the] television giving instructions to deny access to all programming or video exceeding [a] preset ratings limitation.” *Ibid*. This is strikingly similar to how the broadcast flag works, and most importantly, the V-Chip affects the broadcast signal *after* the initial broadcast has completed.

Congress granted the FCC specific authority to regulate a signal *after* its initial reception with regards to the V-Chip. With respect to the Broadcast Flag, it is true that “[congressional] inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction, including the inference that the existing legislation already incorporated the offered change.” *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633 (1990) at 650 (internal quotation marks omitted). In this case however, the inference that existing legislation is sufficient to give the FCC jurisdiction is most plausible. Not only has the Supreme Court allowed the jurisdiction of the FCC to exceed the point of initial reception of a broadcast (see *Southwestern Cable* supra), but Congress has shown through other legislation that it believes the FCC’s jurisdiction goes beyond the initial reception as well (see V-Chip legislation supra). “...[It] is clear that Congress meant to confer broad authority on the [FCC] so as to maintain, through appropriate administrative control, a grip on the dynamic aspects of radio transmission.” *FCC v. Midwest Video Corp.*, 440 U.S. 689 (1979) at 690.

III. ALTHOUGH FIRST AMENDMENT ISSUES ARE OUTSIDE THE SCOPE OF CERTIORARI, THE DMCA TARGETS ONLY NON-SPEECH ELEMENTS OF COMPUTER CODE AND, THEREFORE, FAIR USE CONCERNS ARE NOT IMPLICATED, BY THE STATUTE

This court does not ordinarily review an issue not granted certiorari. See generally, *Yee v. City of Escondido*, 503 U.S. 519 (1992). Since this case does not represent an extraordinary set of circumstances justifying review of First Amendment issues, such issues should not be reviewed here. Nonetheless, to the extent the First Amendment issue bears on the Court’s analysis for determining whether the FCC’s ancillary jurisdiction includes the ability to mandate use of the Broadcast Flag, the Court should give little weight to any First Amendment concerns because the DMCA does not implicate the First Amendment. In *Universal City Studios, Inc. v. Corley* the Second Circuit found that the DMCA implicated only non-speech aspects of encryption technology code. 273 F.3d 429 (2d Cir. 2001). See also, *RIAA v. Verizon*, 257 F. Supp. 2d 244 (DC Cir. 2003); *US v. Elcom Ltd.*, 203 F. Supp 2d 1111 (N.D. CA 2002); and *Universal Studios v. Reimerdes*, 111 F. Supp 2d 294 (S.D. NY 2001). In addition, “legal downstream uses of copyrighted material by customers is not a defense to the software manufacturer’s violation of the provisions of [the anti-circumvention portion of the DMCA].” *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. CA 2004). Thus, any potential fair use by downstream users of copyrighted material cannot justify circumventing the sort of content encryption technology presented in this case.

This court has previously denied review of First Amendment claims regarding the FCC’s jurisdiction. See *Midwest Video Corp* 440 U.S. 689, see also *CBS v. FCC*, 629 F.2d 1 (DC Cir. 1980). Ultimately, any mandate to implement the Broadcast Flag cannot be seen as the FCC exercising any control over actual content. In the end, it is the content providers who will set the permissions of use for their content and, as such, the FCC is not restricting speech with its regulations in this case. In fact, it was the content providers, not the FCC, who “asserted that they will not permit high quality programming to be broadcast digitally” without some sort of protection like the Broadcast Flag. Flag order 17 FCCR 16027. Such control over content has simply not been mandated by the FCC.

CONCLUSION

For the foregoing reasons, the lower courts decision must stand, and the decision of the DC circuit in *Am. Library Ass'n v. FCC* must be overturned.