

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 PETITIONERS
DANIEL BALTIMORE, ET AL.**

OREN BITAN
LOYOLA LAW SCHOOL
919 Albany Street
Los Angeles, California 90015-1211
(213) 453-6951

FRANKLIN JIRÓN
CALIFORNIA INSTITUTE OF TECHNOLOGY
1200 East California Boulevard
Pasadena, California 91125
(626) 395-6811

MICHAEL W. FITZGERALD
CORBIN & FITZGERALD LLP
601 West Fifth Street, Suite 1150
Los Angeles California 90071-2024
(213) 612-0001

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 demodulating devices by requiring recognition of the broadcast flag?

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

Pursuant to Rule 14.1(b), the parties to the proceeding are fully listed in the United States' petitioners' brief. Petitioners juxtaposed have no parent company, and no publicly traded company owns 10% or more of its stock. The named defendants in the underlying district court cases—but not parties to the particular district court ruling at issue on certiorari review here—include Cal Tech, which is not publicly traded and has no parent companies, subsidiaries or affiliates that have issued shares to the public. Cal-tech is a nonprofit educational organization of approximately 5,000 students, professors, and support staff. Cal-tech is dedicated to educating the next generation of engineers, economists, and computer programmers. Cal-tech is dedicated to promoting information services and the public's right to a free and open information society.

TABLE OF CONTENTS

| | <u>Page</u> |
|---|-------------|
| QUESTIONS PRESENTED | i |
| PARTIES TO THE CASE AND RULE 29.6 STATEMENT..... | ii |
| TABLE OF CONTENTS | iii |
| TABLE OF AUTHORITIES | iv |
| OPINION BELOW | 1 |
| JURISDICTION | 1 |
| STATEMENT OF FACTS | 1 |
| SUMMARY OF ARGUMENT | 3 |
| ARGUMENT | 5 |
| I. 5C ENCRYPTION IS NOT EFFECTIVE WITHIN THE MEANING OF THE DMCA..... | 5 |
| A. Underlying 5C encryption is not effective..... | 5 |
| B. In light of technological advancement, 5C does not protect against the common user..... | 7 |
| C. Economic efficiency suggests that 5C technology needs to be replaced..... | 8 |
| II. THE FCC DOES NOT HAVE JURISDICTION TO IMPLEMENT THE BROADCAST FLAG BECAUSE CONGRESS HAS NOT GIVEN IT THE WIDE AUTHORITY REQUIRED TO REGULATE ALL DEMODULATING DEVICES..... | 9 |
| A. The FCC’s General Jurisdiction Does Not Allow it to Implement the Broadcast Flag..... | 9 |
| B. The FCC’s Ancillary Jurisdiction Does Not Allow it to Implement the Broadcast Flag | 11 |
| C. Congress Has Foreclosed the FCC’s Ability to Regulate Demodulating Devices..... | 12 |
| III. CONGRESS CANNOT DELEGATE THE FCC POWER TO IMPLEMENT THE BROADCAST FLAG BECAUSE IT IS TOO BROAD AND DOES NOT PROTECT ESTABLISHED FIRST AMENDMENT AND FAIR USE RIGHTS | 12 |
| A. Congress Cannot Delegate Broad Authority to the FCC that Restricts Fair Use and Educational Rights..... | 12 |
| B. Congress Cannot Delegate Broad Authority to the FCC that Limits Speech..... | 13 |
| 1. Computer Code is Protected Speech..... | 14 |
| 2. Compilation of Ideas is Protected Speech..... | 15 |
| CONCLUSION | 17 |

TABLE OF AUTHORITIES

| <u>SUPREME COURT CASES</u> | <u>Page</u> |
|---|-----------------|
| <i>Associated Press v. United States</i> , 326 U.S. 1 (1945) | 15 |
| <i>Chevron, U.S.A., Inc. v. NRDS, Inc.</i> , 467 U.S. 837 (1984)..... | 9 |
| <i>Community Television of Southern California v. Gottfried</i> , 459 U.S. 498 (1983) | 15 |
| <i>Eldred v. Ashcroft</i> , 537 U.S. 186 (2003) | 15 |
| <i>Harper & Row, Publishers, Inc. v. Nation Enterprises</i> , 471 U.S. 539 (1985) | 15 |
| <i>Hurley v. Irish-American Gay, Lesbian and Bisexual Group</i> , 515 U.S. 557 (1995) | 12, 14 |
| <i>Miami Herald Publishing Co. v. Tornillo</i> , 418 U.S. 241, 258 (1974) | 14 |
| <i>Red Lion Broadcasting Co. v. F.C.C.</i> , 395 U.S. 367 (1969) | 15 |
| <i>Sony v. Universal</i> , 464 U.S. 417 (1984)..... | 15 |
| <i>Staples v. United States</i> , 511 U.S. 600 (1994)..... | 6 |
| <i>Turner Broadcasting System, Inc. v. F.C.C.</i> , 512 U.S. 622 (1994) | 14 |
| <i>U.S. v. Southwestern Cable Co.</i> , 392 U.S. 157 (1968)..... | 10 |
| <u>CIRCUIT CASES</u> | <u>Page</u> |
| <i>Am. Library Ass’n v. F.C.C.</i> , 406 F.3d 689 (D.C. Cir. 2005)..... | 8, 9, 11, 16 |
| <i>Bldg. Owners & Managers Ass’n Int’l v. F.C.C.</i> , 254 F.3d 89 (D.C. Cir. 2001) | 10 |
| <i>California v. F.C.C.</i> , 905 F.2d 1217 (9th Cir. 1990) | 10 |
| <i>Illinois Citizens Committee for Broadcasting v. F.C.C.</i> , 467 F.2d 1397 (7th Cir. 1972) ... | 10 |
| <i>Junger v. Daley</i> , 209 F.3d 481 (6th Cir. 2000) | 13,14 |
| <i>Motion Picture Ass’n of Am. v. F.C.C.</i> , 309 F.3d 796 (D.C. Cir. 2002) | 10 |
| <i>Quincy Cable TV, Inc. v. F.C.C.</i> , 768 F.2d 1434 (D.C. Cir. 1985) | 15 |

TABLE OF AUTHORITIES, cont'd.,

| <u>CIRCUIT CASES, cont'd.</u> | <u>Page</u> |
|--|---------------|
| <i>Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.</i> , 925 F. 2d 174 (7th Cir. 1991).... | 5 |
| <i>Universal Studios, Inc. v. Corley</i> , 273 F3d 429 (2nd Cir. 2001) | 13, 14 |
| | |
| <u>STATUTES, CONSTITUTIONS and LEGISLATIVE MATERIAL</u> | <u>Page</u> |
| U.S. CONST. amend. I..... | 12 |
| U.S. CONST. art. I, § 8..... | 12 |
| 17 U.S.C. §1201 (a)(3)(B)..... | 4, 5 |
| 17 U.S.C. §101..... | 1 |
| 28 U.S.C. §1338(a) and (b)..... | 1 |
| 38 U.S.C. §1254(1)..... | 1 |
| 47 U.S.C. § 151 et seq..... | 9 |
| 18 F.C.C.R. at 23,563..... | 10 |
| Audio Broadcast Flag Licensing Act of 2006, H.R. 4861 (March 2, 2006) | 11 |
| Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218..... | 11 |
| 47 C.F.R. 73.9000-73.9009..... | 11 |
| <i>In the Matter of Digital Broadcast Copy Protection</i> , 17 FCCR 16027..... | 14 |
| <i>In the Matter of Digital Broadcast Copy Protection, Joint Comments of the Motion Picture Association of America, Inc., et. al.</i> , MB Docket No. 02-230, at I. (Dec. 6, 2002), available at http://www.mpaa.org/Press/MPAA_Comments_02-230.pdf | 14 |
| Comments of the Electronic Frontier Foundation Opposing the Broadcast Flag Rule. (Dec 6, 2002), available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513395409 | 5, 11, 13, 14 |

TABLE OF AUTHORITIES, cont'd.,

| <u>MISCELLANEOUS</u> | <u>Page</u> |
|---|-------------|
| Cuong Lam Nguyen, <i>Postmortem Of The Digital Television Broadcast Flag</i> , 42 Hous. L. Rev. 1129, 1148 (2005)..... | 13 |
| Implications of the Broadcast Flag: A Public Interest Primer 10 (2003), Center For Democracy & Technology, <i>available at</i> http://www.cdt.org/copyright/031216broadcastflag.pdf | 10, 14 |
| Intel Homepage, <i>available at</i> https://welcome.intel.com/login.aspx?target= https://ssl.intel.com/ipc-app/default.aspx?lang=eng&ctry=us) | 5 |
| CNN/Reuters, <i>available at</i> http://money.cnn.com/ 2006/03/15/news/international/ sony_ps3.reut/?cnn=yes (last visited March 15, 2006). | 8 |
| International Federation of Phonogram and Videogram Producers Newsletter (IFPI), <i>available at</i> http://www.ifpi.org/site-content/antipiracy/piracy2003-piacy-statistics.html (last visited April 1, 2006) | 8 |

OPINIONS BELOW

The opinion of the district court can be found at 25 Loy. L.A. Ent. L. Rev. 55 (2004), *available at* <http://techlaw.lls.edu/events/atc2004/opinion.pdf>.

JURISDICTION¹

The District Court entered its judgment on May 21, 2004, and had jurisdiction pursuant to the Copyright Act, [17 U.S.C. §§101](#) et seq., and [28 U.S.C. §1338\(a\) and \(b\)](#). The petition for writ of certiorari was timely filed. This Court has jurisdiction under § 1254(1).²

STATEMENT OF FACTS

In the fall of 2003, Professor Sundance Law taught a course called Digital Protection. In this course, he divided the class into two halves matching a student from one half with a counterpart from the other half. One of these students was responsible for writing a digital encryption program, and the other student was assigned to try to break that encryption. In order to facilitate learning and sharing of ideas, all assignments done for the class were posted on the class web page.

One of these student pairs that term was Dmitri Skylore and Jon Johnson. Skylore used both content encryption and copy control information ("CCI") to protect access to copy digital content. The CCI specified the number of copies that could be made of a particular file. Skylore embedded the CCI into the content encryption using 128-bit encryption.

Johnson's assignment was to break Skylore's encryption. Johnson used the idea of programs such as SETI@home, in which a program harnessed the computational power of a large number of personal computers in order to solve a problem more quickly. He posted a distributional program on the class website and invited other Caltech students to download it and to contribute to breaking the encryption. Once the content encryption was bypassed, Johnson simply set the permissions to infinite copies. Johnson posted the results of his brute-force program along with his resume in the hope of getting a lucrative consulting job to help pay for his school tuition.

Professor Law recognized that Skylore's program was similar to "5C" Broadcast Flag technology that many major entertainment corporations are developing [with the exception that 5C used a much weaker 56-bit encryption](#). Professor Law posted a few seconds of 5C encrypted

Comment [FSJ1]: Actually there is an inconsistency with the statement of facts from defense and prosecution to enter whether Skylor's encryption was 56 or 128.

¹ Typically, denials of motions to dismiss are not appealable because they are not considered final judgments. For the purposes of this moot court, however, the district court's denial of defendants' motion to dismiss is considered a final judgment.

² After this unusual appeal, this Court granted certiorari prior to consideration of the case by the Twelfth Circuit.

video on the class website, and Johnson's brute-force program returned the decryption key within a day.

Word spread about Johnson's program, and soon students were going to his website to get the available decryption keys. The entertainment corporations got wind of this website and realized what the decryption keys could potentially do. They decided not to update their encryption algorithms to prevent Johnson's keys from working, or use a higher bit encryption, which they could have done. Instead the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and Intel (co-inventor of "5C" technology) banded together to persuade the Department of Justice to prosecute Jon Johnson, Professor Law, Caltech, and President Daniel Baltimore, who had not been involved at all in the unfolding events thus far. DOJ offered to drop charges in exchange for Caltech removing Johnson's website and prohibiting Prof. Law from teaching students how to decrypt "digital rights management devices or commercial encryption technology now in use or development." The university responded that it would be compromising academic freedom by complying with the government's demand.

SUMMARY OF ARGUMENT

This case is about the difficult balance between copyright protection and consumer rights in an increasingly technological marketplace. Denying compensation to creators and distributors of digital content undermines First Amendment values by stifling expression, threatening the growth of new media and e-commerce, and depriving consumers of a robust marketplace of content offerings. At the same time, resolving these issues should not come at the expense of reasonable consumer expectations regarding the use of copyrighted works and digital technologies. Nor should it come at the expense of the Internet and innovative new communications technologies that hold tremendous promise to promote free expression, economic growth and civic discourse.

In order for a copyright protection technology to be protected by the Digital Millennium Copyright Act (DMCA), the statute clearly states that the technology used must be effective. The standard for determining if such a technology is effective must take into account current industry standards and also consider technological advancements in the near future. A copyright protection technology should only be considered effective if and only if it adheres to minimum industry standards while at the same time be able to show a good faith effort to resist circumvention in light of technological advancement.

The 5C Digital Transmission Content Protection technology (DTCP) used in the ATSC “broadcast flag” is not effective because it uses outdated 56-bit encryption technology that is no longer industry standard and will be easily circumvented using technology from the near future. Furthermore, it is economically efficient to force copyright holders to implement a minimum standard of effectiveness in their protection technology so as free the courts from unnecessary, numerous overwhelming circumvention claims. Industry has abandoned 56-bit encryption as they expect this standard to be easily defeated and thus any copyright holder with foresight must implement a higher encryption standard. Failure to do so is a mistake this Court must not tolerate so as to protect both the economy and the caseloads of the district courts. This case, in which academic innovators face the specter of federal prosecution, illustrates the dangers to which the statute can give rise unless properly interpreted by this Court.

The Federal Communications Commission (“FCC”) attempted to set the standard for digital television (“DTV”) broadcasts by proposing the broadcast flag regime. The flag appeals to movie studios because it digitally locks DTV broadcasts to safeguard against illegal redistribution of television content. Under the proposed FCC order, the flag would be required on all new televisions, DVD players, computers, and any other device that could receive or playback television content. The flag puts the FCC in the position to approve devices and uses before their use, including activities protected by fair use and educational exemptions. As technologies evolve, educators’ and consumers’ access to information should also evolve. The broadcast flag, however, could limit the expansion of educators’ and consumers’ access to information by restricting time and place shifting. Moreover, the public’s right to receive information is protected by the First Amendment. As a result, educators’ and consumers’ speech could be unreasonably limited by the broadcast flag.

In addition, the flag affects personally programmed devices. All computer networks capable of playing television, built by novice and student computer programmers, would be outlawed unless approved by the FCC. Student networks use open source code, and evolving First Amendment jurisprudence has protected computer code as speech. As a result, the broadcast flag could create an unconstitutional prior restraint on the First Amendment rights of private home programmers.

The District of Columbia Court of Appeals, however, struck down the proposed broadcast flag because it exceeded the FCC's ancillary jurisdiction. *American Library Association v. F.C.C.*, 406 F.3d 689 (D.C. Cir. 2005). The FCC has never attempted to regulate playback devices. To justify this expansion of power, the FCC reasoned that the broadcast flag was necessary to assure content makers that their copyrighted material would be protected against digital piracy. The court rejected the FCC's argument, and Congress is considering granting the FCC additional power through targeted legislation. As a result, the indictment against petitioners should be dismissed until these issues are resolved.

ARGUMENT

I. 5C ENCRYPTION IS NOT EFFECTIVE WITHIN THE MEANING OF THE DMCA.

A. Underlying 5C Encryption is not Effective.

The effectiveness of a system designed to protect digital content can be measured by simply noting the difficulty that an unauthorized user has in accessing the. Encryption is by far the most widely used protection scheme used in industry. This technique turns a piece of data (i.e. a movie clip) into unintelligible data that can be turned back into the original data if the correct password is used, much like having the correct numeric combination for a safe deposit box. Obviously, the longer the combination for a safe, the harder it would be for an individual to correctly guess the password (or brute-force attack) and claim the prize within. The same applies in encryption where content is protected by a password called a key. This key is made up of the most basic data a computer can understand, one and zeros, or a “bit.” The more bits are used in a key, the harder it will be for a “hacker” to unscramble the desired content. Everyday things like credit card transactions and website passwords are encrypted with a modern 128-bit encryption. From all of this, one must ask the question: if 128-bit encryption is good, why not use 256 or 1 million-bit encryption? The simple answer is that it would be too hard and cost too much to protect something with that much encryption. This would be the equivalent of the United States using using a nuclear missile to guard a \$100 bill. However, at the same time it would not be out of the question to use a \$5 lock to secure the bill.

Specific to our case, the defendants are accused of violating the Digital Millennium Copyright Act (“DMCA”), a law that makes it illegal for anyone to “manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that...is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner to a work protected under this title in a work or portion thereof.” 17 U.S.C. § 1201. The defendants are accused of circumventing the 5C encryption technology planned to be used in the broadcast flag. This flag would signal a device to encrypt media using 5C technology so as to protect it from unauthorized copying. This is the equivalent of using a squirt gun to guard that \$100 bill.

At the heart of the 5C encryption technology is the use of an ineffective 56-bit key. As the expert witness for the defense testified, “symmetric ciphers with key lengths around 56 bits and below should be considered ‘weak’ and not deployed in new applications.” In 2004, the National Institute of Standards and Technology (NIST) declared that the 56-bit encryption previously used was no longer secure enough to protect government information. This is of course in clear contrast with the requirement that any DRM technology protected under the DMCA must be “effective”.

As previously stated, the industry standard in consumer encryption technology is the use of at least a 128-bit encryption. There has been a widespread upgrade from 56 to 128-bit protection across government and retail. Even the websites for the companies that developed the

5C technology use 128-bit encryption³. These entities cannot claim that 56-bit encryption is effective when they themselves use higher encryption standards for daily operations. It is quite unclear why a lower key length for this technology was used when there were serious doubts about its security. The Court cannot protect a DRM technology that was not created in good faith, sincere effort to thwart infringers. The 5C technology could have been made stronger.

It is also worth noting that much like the DeCSS technology used to protect DVD's, 5C relevant keys and other information are published with every implementation of the technology [cite defense witness]. Although this Court has ruled in the past that distribution of secret information does not imply giving up protected rights, *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*, 925 F.2d 174 (7th Cir. 1994), the court required that this disclosed secret information be necessary for the normal functioning of the product. In the case of DRM technologies, this is not necessary and thus inclusion of sensitive information such as unprotected keys should be regarded as a weakness. In DRM system used by Apple, FairPlay, most keys are stored on internet servers while keys that are on the local machines are also further encrypted.

Lastly we ask the Court to consider the framework under which the 5C technology is being proposed and find that the effectiveness of the encryption is moot since other factors make it ineffective. As described by the EFF, "it will always be easy to build or acquire non-compliant devices." [Comments of the Electronic Frontier Foundation Opposing the Broadcast Flag Rule](http://www.eff.org/Commentary/2002/12/06/efn-021206-01). (Dec 6, 2002) (available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513395409). If a device that does not implement the broadcast flag is used, the received media is not encrypted in the first place. Anyone who wishes to circumvent the broadcast flag would not bother to decrypt content using the defendant's work, but would rather bypass the initial encryption by building or using a non-compliant device. Overall, the proposed implementation framework for the 5C technology is not effective and therefore any of its components should not be eligible for DMCA protections.

In determining the effectiveness of the copyright protection technology the district court considered the statutory definition of effective under the DMCA. The Court found that the technology does not need to make circumvention impossible, but rather "in the ordinary course of its operation, requires the application of information, or processes, or a treatment, with the authority of the copyright owner, to gain access to the work" in order for it to be considered effective. 17 U.S.C. § 1201 (a)(3)(B). The district court found that a plain reading of the statute would consider effective the most minimal application of processes, and treatments designed to protect copyrightable work. The court further stated that even if a more narrow definition was used such that the protection measure is required to "operate reasonably to control access to copyrightable material," the 5C technology would still be considered effective because "extraordinary efforts are required to bypass the protection system. We assert that the technology in question does not require unreasonable and extraordinary efforts to be bypassed

³ For example Intel uses RC4 128-bit encryption for their login pages (<https://welcome.intel.com/login.aspx?target=https://ssl.intel.com/ipc-app/default.aspx?lang=eng&ctry=us>)

⁴ The case dealt with a company distributing schematics that they wanted to keep as a trade secret because it was necessary for the operation of the device. Their trade secret was protected by the court because there was no inadequate protection found since it was necessary for to publish the design.

since it uses weak encryption and does not protect against the common user. Furthermore, the district court was incorrect in upholding the least restrictive definition of effective as this goes against the rule of lenity established by this Court. The doctrine states that an “ambiguous criminal statute is to be construed in favor of the accused” and therefore the lower court should have used the more restrictive definition which the 5C technology does not meet. *See Staples v. United States*, 511 U.S. 600, 619, n. 17 (1994).

B. In Light of Technological Advancement, 5C Does not Protect Against Common Users.

Although it is clear that 5C encryption did not use the standard minimum encryption at the time of development, and that this could have been corrected, the Court must also determine if this update was truly necessary in order for the technology to be considered effective. The original motion to dismiss was denied on the grounds that the defendants had uncommon technical skills and access to large computing power not available to the common user. Even with the 56-bit encryption it took at least a day for cipher keys to be broken using the defendant’s program. The district court found that the “encryption prevents access to all except a few skilled people” [cite correctly] and thus the technology was effective. We believe that this opinion did not consider current and future technological trends.

As stated by the expert witness for the defense, “the processor power available to an attacker for a constant cost would also tend to double every eighteen months because of improvements in technology.” This also does not include the recent trend in the popularization of distributive computing projects that will make the networking of computers across the internet for the purpose of solving specific problems easy. A preliminary internet search⁵ comes up with over 50 such projects such as SETI@Home.⁶ In short, the computing power available to the common user is growing at an extraordinary rate. No company using outdated 56-bit encryption can truly believe that their product is going to be secure for very long. This is in direct contrast to prosecutions expert witness claim that the “system can only be circumvented by knowledgeable professional technicians with massive processing power who approach the DRM with the intent of illegally cracking the encryption.”[cite correctly] Not only is the level of security used by the technology sub par, so as to make non-professional technicians able to crack it, but the defendants cannot be characterized as individuals bent on illegal cracking. The Court must remember that the circumvention was done under the backdrop of education, research, and innovation.

The district court also argued that significant technological skills are needed to splice the “cracked” video files into a single movie. Video editing has been a booming business. Anyone with Microsoft’s five-year-old Windows XP operating system has basic video editing capabilities built-in capable of doing this splicing. Technology improvement in the near future will enable the common user to deploy sophisticated encryption cracking and video editing techniques with ease.

⁵ For a comprehensive list see <http://www.distributedcomputing.info/projects.html>

⁶ SETI@home (“SETI at home”) is a distributed computing project for Internet-connected home computers, hosted by the Space Sciences Laboratory, at the University of California, Berkeley, in the United States. SETI is an acronym for the Search for Extra-Terrestrial Intelligence.

In summary, the district court underestimated the computing power available to the modern consumer, and furthermore assumed that they lacked basic video editing skills. Although, the idea of distributing computing was novel a few years ago, we have seen a strong trend towards mainstream. Even without this leap in computing power, a single personal computer will be able to more easily crack weak 56-bit encryption each year. In light of a fast paced technology available to consumers, there is no reason that that the 5C technology should have relied on outdated encryption methods. This technology does not “reasonably control access” to the copyrighted media nor does it require “extraordinary efforts” to bypass it.

C. Economic Efficiency Suggests that 5C Technology Needs to be Replaced.

With any given encryption technology there will always somebody who is smart enough to circumvent and there will eventually be enough technological advancement to make circumvention by the common user trivial. Given this constant trend of DRM technologies failing to protect content, how can any DRM technology truly be considered effective?

Much like torts, a system must be setup in digital copyrights protection technology that will give rise to the most economically efficient outcome. In torts, a delicate balance is struck between the liability of the consumer and the retailer. Imagine a store that is 100% liable for any accidents that occur to customers on its property. This policy would encourage the consumer to be careless in the store and the store owner to implement every imaginable safety feature so as to prevent any physical harm to the customer. We would see padded walls and extra-grip floor so as to prevent falling. Soon the cost to ensure safety for the customer would be too high and the store will go out of business. Alternatively, a policy that makes customers 100% liable for any accidents on store property would encourage negligent store owners with wet, slippery, unsafe stores. In the end, the customer would be so afraid of being hurt in the store that he would stop shopping at the store resulting in its bankruptcy. Both scenarios describe an economically inefficient system. There must be a reasonable balance between what the store owner and the costumer are liable for so as to ensure the business remains open.

DRM technologies must also be placed in a balance framework that will encourage economic efficiency. It will cost too much for a company to develop a million-bit encryption that guarantees total security. If a system can keep out 99% of consumers from making illegal copies, then laws such as the DMCA can be used to ensure that the remaining 1% will be prosecuted for circumventing. It is cheaper to use the law to prosecute a small number of individuals, than to create a system that nobody can circumvent.

However, in order for this setup to be economically efficient the initial burden to create a DRM technology that is “good enough” must fall squarely on industry and not the courts. DRM technology must be the first line of defense against copyright infringement, and not the law. Lack of development of effective DRM technology will result in a sharp rise of cases that will clog the court system under the DMCA. Companies must be forced to look for innovation that will outdo everyone but a hand full of people that can be controlled with legislation. The research and innovation that DOJ is attacking in this case is what will ensure economic efficiency.

Outside of the DMCA, good DRM is beneficial for copyright holders. Most of the media piracy in the world occurs outside of the United States, well outside the jurisdiction of this court and the DMCA. “The global pirate music market is bigger than any individual national legitimate music market except for the USA and Japan.” See International Federation of Phonogram and Videogram Producers Newsletter (IFPI), *available at* <http://www.ifpi.org/site-content/antipiracy/piracy2003-piacy-statistics.html> (last visited April 1, 2006). A company serious about protecting content will look towards the future with research and innovation and not towards the past with 56-bit encryption.

Recently Sony (one of the 5C companies that developed the technology in question) announced the delay of their much-anticipated PS3 game console due to copyright protection technology concerns. See CNN/Reuters, *available at* http://money.cnn.com/2006/03/15/news/international/sony_ps3.reut/?cnn=yes (last visited March 15, 2006). This has caused Sony a drop on stock price and lost of a market edge by being the last next-generation game console to be shipped. They would not do this if they did not understand how important DRM technology is. The government cannot make the case for the effectiveness the 5C technology when one of the 5C members chooses to lose money to ensure a better standard than the technology in question. The companies whose interests are clearly being protected have the resources to develop better technology, but they chose not to do the economically efficient thing. An error in judgment was made by using ineffective technology, and it is not this Court’s job to fix it.

Allowing the district court decision to stand would create an economically inefficient system where ineffective technologies would be protected. This case represents the first in many future cases involving the 5C technology. The defendants will not be the last to easily bypass the 5C protection scheme. Unless this Court is willing to force lower courts to take on the burden and responsibility of deliberating on countless cases involving people who broke into a safe with a broken lock, the 5C technology as it stands must not enjoy this Court’s protection. These companies should be forced to use current minimum industry encryption standards that will ensure the shrinking of potential defendants the courts will see. The 5C technology is not effective, it will be less effective tomorrow, and gives rise to bad economics. The district court decision must be overturned to ensure economic wellbeing.

II THE FCC DOES NOT HAVE JURISDICTION TO IMPLEMENT THE BROADCAST FLAG BECAUSE CONGRESS HAS NOT GIVEN IT THE WIDE AUTHORITY REQUIRED TO REGULATE ALL DEMODULATING DEVICES

A. The FCC’s General Jurisdiction Does Not Allow it to Implement the Broadcast Flag.

As a preliminary matter, the FCC, in *American Library Association v. Federal Communications Commission*, 406 F.3d 689 (D.C. Cir. 2005), conceded that its general jurisdiction does not allow it to implement the broadcast flag because that authority only allows it to regulate devices while they receive television signals. See *id.* at 692, 708. As a result, the

FCC unsuccessfully relied on its ancillary jurisdiction to justify its implementation of the broadcast flag. *Id.*

This Court in *Chevron, U.S.A. Inc., v. Natural Resources Defense Counsel, Inc.*, 467 U.S. 837 (1984), enunciated a two part test to assess the FCC's powers. The first part looks to Congressional intent. *Id.* at 842-43. "If the intent of Congress is clear," the court must give effect to that intent. *Id.* In the event Congress has not spoken, the second part of the test looks to the FCC's reasonableness. If "Congress has not directly addressed the precise question at issue," the agency's statutory action is entitled to deference, as long as it is reasonable." *Id.*

In *American Library Association v. Federal Communications Commission*, 406 F.3d 689 (D.C. Cir. 2005), the District of Columbia Court of Appeals analyzed what powers Congress delegated to the FCC in the Communications Act of 1934, 47 U.S.C. § 151 et seq. (2000) ("Communications Act" or "Act"), to regulate apparatus that can receive television broadcasts when those apparatus are not engaged in the process of receiving a broadcast transmission. The court held that under either prong of *Chevron* the FCC's exceeded its power when it attempted to implement the broadcast exceeded. *Id.* at 691, 699. The court stressed that its "judgment is the same whether we analyze the FCC's action under the first or second step of *Chevron*. In either situation, the agency's interpretation of the statute is not entitled to deference absent a delegation of authority from Congress to regulate in the areas at issue." *Id.* at 699. As analyzed below, Congress has not delegated the FCC the authority to pass the broadcast flag.

One of the FCC's own members, Commissioner Abernathy, issued a separate statement, in which she expressed her support for the Flag Order, but noted: "I have previously expressed concerns about whether we have jurisdiction to adopt a broadcast flag solution, or whether this is an issue best left for Congress. As a general rule, the Commission should be wary of adopting significant new regulations where Congress has not spoken. . . I am hopeful that any court review of this decision can occur before the effective date of our rules." *Id.* at 695.

The court finally noted that "In the seven decades of its existence, the FCC has never before asserted such sweeping authority. Indeed, in the past, the FCC has informed Congress that it lacked any such authority. In our view, nothing has changed to give the FCC the authority that it now claims." *Id.* at 691.

This Court is not required to follow the D.C. Court of Appeal, but should affirm it due to the negative impact a reversal would cause. The broadcast flag regulates all television content because all programming must carry the flag, yet has no built-in protection for educational and fair uses of any television content. Congress has directly expressed its intent to protect educational and fair uses of content, and is currently debating how to continue to protect fair uses in both audio and video content. *See* Part II *infra*. When Congress previously granted the FCC limited power to regulate content, it did so specifically in the Family Home Entertainment Act.

The FCC's attempt to regulate television content is unreasonable because it goes far beyond its previous regulations, both in the breadth of its regulation and in its impact on consumers and electronics manufacturers. The broadcast flag is the FCC's broadest attempt to regulate electronic devices, and has provoked thousands of complaints from a diverse group of

interested parties including scholars, librarians, computer programmers, and civil libertarians. *See American Library Ass'n. v. F.C.C.*, 406 F.3d 689, 705 (“We recognize that the Commission's assertion of jurisdiction over manufacturers of equipment in the past has typically been tied to specific statutory provisions and that this is the first time the Commission has exercised ancillary jurisdiction over consumer equipment manufacturers in this manner.”) (citing [Flag Order, 18 F.C.C.R. at 23,566](#)); *see* Implications of the Broadcast Flag: A Public Interest Primer (Version 2.0) 10, 30 (2003), available at <http://www.cdt.org/copyright/031216broadcastflag.pdf> (summarizing the unique copyright effects of the broadcast flag)(hereinafter Ctr. for Democracy & Tech). As a result, this Court should dismiss all indictments regarding television content until Congress establishes its policy.

B. The FCC’s Ancillary Jurisdiction Does Not Allow it to Implement the Broadcast Flag.

The broadcast flag was the first time the FCC attempted to exercise ancillary authority over electronics manufacturers. Courts have consistently limited the FCC’s ancillary jurisdiction to television broadcasting, and have rejected arguments attempting to use ancillary jurisdiction to expand the agency’s general powers. *Bldg. Owners & Managers Ass’n Int’l v. F.C.C.*, 254 F.3d 89, 95 n.7 (D.C. Cir. 2001) (striking down FCC’s attempt to regulate placement of satellite dishes); accord *California v. FCC*, 905 F.2d 1217, 1240 n.35 (9th Cir. 1990) (analyzing FCC’s arbitrary decision to expand its jurisdiction).

In striking down the broadcast flag, the District of Columbia Court of Appeal recognized that the FCC may exercise ancillary jurisdiction only when two conditions are satisfied: (1) the Commission’s general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities. *See id.* at 692 (citing 18 F.C.C.R. at 23,563).

As discussed above, the FCC’s general authority does not cover the broadcast flag and its ancillary jurisdiction is too limited to justify such broad regulation. Courts have repeatedly rejected the FCC’s use of ancillary jurisdiction to regulate new areas. In *Motion Picture Ass’n of Am. v. FCC*, 309 F.3d 796 (D.C. Cir. 2002), the D.C. Court of Appeal rejected the FCC’s attempt to regulate television programs under its ancillary jurisdiction. *Id.* at 798. The court also noted that “[t]he FCC cannot act in the ‘public interest’ if the agency does not otherwise have the authority to promulgate the regulations at issue.” *Id.* at 806.

In *Illinois Citizens Committee for Broadcasting v. FCC*, 467 F.2d 1397 (7th Cir. 1972), the Seventh Circuit held that the FCC lacked ancillary authority over objects that interfere with television transmissions. The court noted that when courts have allowed the FCC to assert ancillary jurisdiction, the court explained, they have “tread[ed] lightly even where the activity at issue easily falls within ‘communication by wire or radio.’” *Id.* at 1400.

The broadcast flag, like the FCC’s actions in *MPAA* and *Illinois Citizens*, is too broad to be justified under the FCC’s ancillary jurisdiction. In *United States v. Southwestern Cable Co.*, 392 U.S. 157 (1968), this Court held that the FCC could regulate television antennas to help ensure increased access to content. The regulation at issue was different than the broadcast flag

because antennas do not alter consumer and educational uses of television content, but the broadcast flag does. In addition, regulations over television antennas are different in scope than the power to regulate all demodulating devices, effectively regulating every media device in the home. With increased integration between devices, the broadcast flag could give the FCC the power to control every device in the house, even kitchen appliances that are plugged into home networks. As the D.C. Court of Appeal reasoned, there must be a boundary to limit the FCC's power, and the agency's authority is limited to devices that directly receive transmissions. *Am. Lib. Ass'n v. F.C.C.*, 406 F.3d at 707.

C. Congress Has Foreclosed the FCC's Ability to Regulate Demodulating Devices.

In striking down the broadcast flag, the D.C. Court of Appeal noted that it "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." *Am. Lib. Ass'n v. FCC*, 406 F.3d at 704. Rather than grant the FCC broad powers, Congress has recently granted the FCC limited authority in specifically drafted laws.

To regulate family friendly content like the V-Chip, Congress specifically authorized the FCC to do so with the Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218 (April 27, 2005). Without that grant of power, the V-Chip, like the broadcast flag, would have exceeded the FCC's powers.

In addition, after growing debate about fair use and educational rights, the House of Representatives recently introduced the Audio Broadcast Flag Licensing Act Of 2006. Introduced in the House on 03/02/06, this bill narrowly authorizes the FCC to impose licensing conditions on digital audio radio to protect against the unauthorized distribution of transmitted content.

III CONGRESS CANNOT DELEGATE THE FCC POWER TO IMPLEMENT THE BROADCAST FLAG BECAUSE IT IS TOO BROAD AND DOES NOT PROTECT ESTABLISHED FIRST AMENDMENT AND FAIR USE RIGHTS.

A. Congress Cannot Delegate Broad Authority to the FCC that Restricts Fair Use and Educational Rights.

Even if this Court decides that the FCC acted within its authority to pass the broadcast flag, petitioners' indictments should still be dismissed because of the larger implications of this type of copyright enforcement. The broadcast flag aims at a copyright problem, studios' fear of indiscriminate redistribution of their copyrighted content, but it is not typical copyright law. Digital Broadcast Content Protection, [68 Fed. Reg. 67,599](#) (Dec. 3, 2003) (codified at [47 C.F.R. 73.9000-73.9009 \(2004\)](#)) (justifying the broadcast flag as necessary "to preserve the viability of over-the-air broadcasting" from the threat of illegal internet redistribution."); *See also* Ctr. for Democracy & Tech at 30. Instead of focusing on infringing uses of DTV broadcasts like taping a show and selling copies, this new kind of regulation puts the government in the business of redesigning products that might be used to infringe. *Id.* In the process, it locks out many non-

infringing uses, including fair uses of copyright, innovative technologies, and educational software developers. Because these collateral harms are unavoidable, technology mandates should be a last resort, not a predictive strike against hypothetical danger.

The broadcast flag affects consumers by indiscriminately restricting uses of broadcast programming, and does so regardless of whether these programs are entitled to copyright protection, or are even copyrightable. EFF Comments Opposing Broadcast Flag, J.A. 721. For example, if the broadcast flag is implemented, students and professors will not be able to send any portion of a flagged DTV broadcast over the Internet for any reason. *Id.*

Under the flag, professors or judges could not e-mail a clip of a DTV broadcast to an office, second home, or traveling family member, even if the clip was uncopyrighted or it was newsworthy, like the State of the Union Address. *Id.* In addition, law students and professors could not use any clip that has been marked with the flag to make, illustrate, or rebut an argument in an Internet discussion group, website, or "blog." Moreover, consumers could not share a clip of a DTV broadcast with a virtual classroom during a distance learning lesson, or create original works using the DTV broadcasts in ways that have not yet been conceived. No one may be able to fully assess the extent of this loss, since the new rule will halt creativity and innovation before it can blossom.

The technical specifications of the broadcast flag mandate do not explicitly foreclose fair use copying. Indeed, the FCC has repeatedly stated that "our goal of preventing the indiscriminate redistribution of digital broadcast TV content 'will not (1) interfere with or preclude consumers from copying broadcast programming and using or redistributing it within the home or similar personal environment as consistent with copyright law.'" But much fair use copying falls into the gap between the rule and its implementation. Moreover, the flag could chill public debate and access to information in violation of the First Amendment's protection of free speech.

B. Congress Cannot Delegate Broad Authority to the FCC that Limits Protected Speech.

If Congress delegated narrow authority to the FCC to pass a broadcast flag, the FCC and Congress would still be limited by the First Amendment. The broadcast flag limits educational speech, consumers' right to edit and compile content, and the educational and privately generated computer code. The First Amendment to the Constitution states "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I. This Court has expressed that the scope of the First Amendment is versatile; the artwork of Jackson Pollack, the music of Arnold Schoenberg, or the Jabberwocky verse of Lewis Carroll are "unquestionably shielded." *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*, 515 U.S. 557, 569 (1995). In addition, the First Amendment establishes that access to information is a fundamental value of the American political system. *Id.*

1. Computer Code is Protected Speech.

Respondents stress the dangers of internet piracy as justification for the FCC's broad based regulations. It is true that computers and the Internet have made it much easier for users from around the world to illegally digitize and then share television and music content. Proponents of the broadcast flag, such as the MPAA, argue that because computers are the primary facilitators of digital piracy, policymakers should adopt more stringent robustness standards to ensure computer compliance. *See* Cuong Lam Nguyen, *Postmortem Of The Digital Television Broadcast Flag*, 42 *Hous. L. Rev.* 1129, 1148 (2005). Policymakers should consider computers as a special case, but not for the reasons advanced by broadcast flag proponents. Broadcast flag regulations would have limited the valuable participation of open-architecture devices, such as computers, in the digital transition. Computers are essential to digital evolution because a computer's open-architecture is a common outlet for protected first amendment speech.

5C protection technology, as discussed above, does not allow transmission of flagged content to a computer through a digital connection unless all of the computer's digital outputs are secure digital outputs. *Id.* at 1140. This restriction precludes interoperability between current computers and future broadcast flag-compliant devices. High Definition Television ("HDTV") tuner cards and Digital to Audio converters allow users to create personal networks that enable time and place shifting within their homes and personal devices. *See* Fred Von Lohman. Individual programming is necessary to operate these home networks. *Id.* In addition, students and private programmers use open source code to design programs that function in similar ways as commercially available encoding programs. *Id.* Under the broadcast flag, any individual programming for devices that receive or transmit content is prohibited unless it contains and recognizes the broadcast flag in a way previously approved by the FCC. *Id.*

This Court has yet to analyze computer code as First Amendment speech. Lower courts, however, have held that computer code is protected speech. *Universal Studios, Inc. v. Corley*, 273 F3d 429 (2nd Cir. 2001); *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000) (holding computer code is protected speech even if a computer is required to understand its expression or function)). As a result, students and professors that program software are protected by the First Amendment, as set forth below.

In *Junger v. Daley*, 209 F3d 481 (6th Cir. 2000), the Sixth Circuit Court of Appeals analyzed whether computer source code falls under First Amendment protection. *Id.*; *see also Universal Studios, Inc. v. Corley*, 273 F3d 429 (2nd Cir. 2001). The plaintiff, Professor Peter Junger, facially challenged provisions of the Export Administration Regulations that banned exports of encryption software. *Id.* The court held that even non-traditional speech like musical scores and computer source code, although not understood by the majority of people, are still protected by the First Amendment because they express information and ideas within their respective fields. *Id.* at 484. Although the court differentiated between functional and expressive speech, and noted that limits on functional speech would receive less scrutiny, it stressed that both forms of speech and hybrid forms still receive First Amendment protection. *Id.* Functional speech is also a key technological tool that helps express other forms of speech.

In *Universal Studios v. Corley*, 273 F3d 429 (2nd Cir. 2001), the Second Circuit also analyzed the difference between functional and expressive speech. The lawsuit was brought by the motion picture studios under the Digital Millennium Copyright Act to enjoin defendants from posting or downloading software that decrypted DVDs. *Id.* The court upheld the injunction, holding that computer code does receive First Amendment protection. *Id.* at 432. However, the court also found that defendants' decryption software functioned solely to circumvent technological locks on DVDs, and defendants were not posting the code as an educational exercise. Therefore, after balancing the parties' interest, the court held that the speech was unprotected due to its capacity to promote piracy. *Id.*

The court did not mention decryption software for personal or educational use. In addition, the court held that the injunction did not ban more speech than was necessary to further the government's interest to prevent piracy. As a result, personal and educational uses of code should be protected by this Court under the First Amendment.

Student and personal programming, like DVD decryption software, has both functional and expressive components. *See* Fred Von Lohman. Students create software during the course of their studies. Personal programmers use code to facilitate time and place shifting of television content. *Id.* Unlike the defendants in *Junger* and *Corley*, however, students and home programmers should receive added protections because they serve a public function. *Id.* Student and private innovators create products that increase the public's access to information. *Id.* As described below, the public's access to information is a paramount importance.

It would be inconsistent for this Court to allow the FCC to shut down educational uses that facilitate lawful uses because it is contrary to Congress' intentions and to the First Amendment. The broadcast flag would shut down all educational and personal uses unless pre-approved by the FCC. *Id.* It also would outlaw consumers and educators that program code for commercially approved devices that did not interact with each other. *Id.* As a result, if this Court does not protect educational and personal, the public's First Amendment and fair use rights will be limited.

2. Compilation of Ideas is Protected Speech.

Access to the media is an important right protected by the First Amendment. An informed public is essential to political discussion, elections, and in maintaining globally competitive levels of education. With the advent of digital media, the public increasingly gets information in more diverse forms, places and methods than ever before. *See Center for Democracy & Tech* at 30 (noting how consumers' access to digital media may be hindered by the broadcast flag). As a result of new technologies that allow for more personalized and portable content, copyright holders are increasingly fearful they lack the control to regulate the new media expansion. *See In the Matter of Digital Broadcast Copy Protection, Joint Comments of the Motion Picture Association of America, Inc., et. al., MB Docket No. 02-230, at I. (Dec. 6, 2002), available at http://www.mpa.org/Press/MPAA_Comments_02-230.pdf.*

First Amendment protection does not require a speaker to generate, as an original matter, each item featured in the communication. *Hurley v. Irish-American Gay, Lesbian and Bisexual*

Group, 515 U.S. at 570. Cable operators, for example, engage in protected speech activities even when they select programming originally produced by others. *Id.* (citing *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 636 (1994) ("Cable programmers and cable operators engage in and transmit speech, and they are entitled to the protection of the speech and press provisions of the First Amendment.")). In addition, edited compilations of speech is a staple of most newspapers' opinion pages, which fall within First Amendment security. *Id.* (citing *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241, 258 (1974)).

Moreover, this Court has repeatedly held that the public has a First Amendment right to receive information. *Id.* The right to receive information is especially significant in electronic media. Although this Court has upheld restrictions where there is scarcity in the broadcasting spectrum, digital television does not pose a scarcity issue because of its increased bandwidth. In *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969), this Court stated: "It is the right of the viewers and listeners, not the right of the broadcasters, which is paramount. . . . It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences which is crucial here." *Id.* at 390.

In *Quincy Cable TV, Inc. v. FCC*, 768 F.2d 1434 (D.C. Cir. 1985), the D.C. Circuit Court of Appeals cited *Red Lion* for the proposition that "the interests of viewers should be considered 'paramount' in the First Amendment calculus." *Id.* at 1445. In response to cases brought by Turner Broadcasting System, the court struck down, as a violation of the First Amendment, the FCC's "must carry" rules. *Id.* These rules required cable systems to carry all local broadcast stations upon their request and without compensation, without regard for the channel capacity of the system or the alternative viewing choices foreclosed as a result. *Id.* The court recognized that the "must carry" rules prevented cable subscribers from receiving cable networks' information and entertainment programming services, although such programming might be preferred over that carried by local broadcast stations. *Id.*

This Court, in *Sony v. Universal*, 464 U.S. 417 (1984), concluded that time-shifting is worthy of protection because the public's expanded access to information, made possible by new technologies, is accorded great weight. Although this Court did not directly cite any of its classic First Amendment cases to support its holding, it did, however, cite its 1983 decision in *Community Television of Southern California v. Gottfried*, 459 U.S. 498, 508 (1983), as to "the public interest in making television broadcasting more available." *Sony*, 464 U.S. at 454. This view bears a strong resemblance to language from several landmark First Amendment cases, such as *Associated Press v. United States*, 326 U.S. 1, 20 (1945), ("[First Amendment] . . . rests on the assumption that the widest possible dissemination from diverse and antagonistic sources is essential to the welfare of the public"), and *Red Lion* ("It is the right of the public to receive suitable access to . . . ideas and experiences which is crucial . . ."). *Red Lion Broadcasting Co. v. FCC*, 395 U.S. at 390. This Court's language in *Sony* also bears a striking similarity to its own earlier summary of the district court opinion in that case. Moreover, the court found that the purpose of this [time-shifting] use served *the public interest in increasing access to television programming*, an interest that "is consistent with the First Amendment policy of providing the fullest possible access to information through the public airwaves." *Id.*

This Court in *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539 (1985), however, made clear that the importance of receiving particular information, standing alone, does not justify copying that adversely affects the marketability of the work. *Id.* at 542. The case involved President Gerald Ford's memoirs. *Id.* The publishers and copyright holders, Harper & Row and Reader's Digest, intended to release the memoirs as a book but sold prepublication excerpts exclusively to *Time* magazine. *Id.* As a result, marketability is a large factor in determining protected consumer uses, but as discussed above, it is not the only factor to consider when analyzing consumer rights.

This Court's most recent analysis of the intersection of the First Amendment and fair use was in *Eldred v. Ashcroft*, 537 U.S. 186 (2003), where the court held that the First Amendment was embedded in consumers' established fair use and educational rights. *Id.* at 220. The court rejected Petitioners' argument that the Copyright Extension Act violated the First Amendment but stressed that the First Amendment is protected by educational and fair uses. *Id.* The broadcast flag, however, does not protect fair use rights or educational rights. Instead, the FCC is put in the position of defining these constitutionally protected rights, and Congress never intended for the FCC to define the public's constitutional rights.

CONCLUSION

For the foregoing reasons, the lower court's decision to deny the motion to dismiss should be reversed, and the District of Columbia Circuit's decision in *American Library Association v. F.C.C.*, 406 F.3d 689 (D.C. Cir. 2005), should be affirmed.