Implications of the Broadcast Flag: A Public Interest Primer (version 2.0)

A Report of the
Center for Democracy and Technology

December 2003

Rev. 2.0

Table of Contents

Note on Version 2.0: After CDT's publication of its October 2003 report Implications of the Broadcast Flag: A Public Interest Primer, *the FCC issued its Final Report and Order adopting the broadcast flag approach (officially published in the* Federal Register *December 2003.) This report updates CDT's earlier report, providing a detailed analysis of the FCC ruling rather than the flag proposals that had been put forward as of October.*

The Center for Democracy & Technology is a non-profit, non-partisan public interest organization dedicated to advancing civil liberties and democratic values on the Internet and other new digital media.

This report was researched, written, and produced with the generous support of the John D. and Catherine T. MacArthur Foundation, the Glushko-Samuelson Foundation, and other CDT supporters.

1634 I Street, NW Suite 1100
Washington DC 20006
(202) 637-9800
(202) 637-0968 (fax)
http://www.cdt.org

1. INTRODUCTION AND OVERVIEW

We are in the midst of a far-reaching civic debate about the legal and technical methods by which copyrighted works will be protected in the digital age. This debate has important consequences for the future of key elements of the US economy: producers of digital content, whose substantial economic interests are at stake; information technology and consumer electronics manufacturers, who would like to bring out new products; and individuals who want choices of devices and access to desirable content. The outcome of the debate will implicate important public values including the free flow of information, access to educational and news content, and technological innovation.

The "broadcast flag" system—a combination of technical standards and federal regulations designed to curtail unauthorized redistribution of digital television broadcasts—has emerged in 2003 as a focal point in the digital copyright debate. Pressure for protection of digital video content has mounted as the U.S. moves steadily towards the transition to digital television called for by 2006. In November 2003, the Federal Communications Commission (FCC) approved a rule mandating that all DTV devices sold after July 2005 incorporate governmentally approved content protection technologies in accordance with the flag scheme. The Commission's ruling left several key issues unresolved, however, and the FCC has initiated a second rulemaking process to address these outstanding issues.[1] In addition, legal challenges to the rule are expected.

In light of the FCC's ruling, the flag debate is proceeding on three levels: (1) on the handling of issues addressed in the FCC's initial ruling; (2) on issues deferred by the FCC to its follow-on rulemaking and (3) on other important issues that the FCC has not explicitly acknowledged but that are already being discussed in other fora or will be discussed in the follow-on proceeding.

The creators of television programming and movies view the broadcast flag scheme as essential to protecting high-quality content distributed through unprotected digital television broadcasts. At the same time, the broadcast flag regulations could have a profound effect on the ability of consumers to watch, record, or use digital television and on the design of devices that play, transmit, or store digital content, including computers.

CDT, along with its partners Public Knowledge and Consumers Union, has conducted in-depth interviews with over 30 of the key stakeholders in the ongoing debate over the broadcast flag. Almost without exception, participants agreed on the importance of three key priorities: protecting copyright and rewarding creators; supporting innovation in new products; and protecting reasonable public uses of content and access to information. There remain serious disagreements, however, on how to implement copyright protection mechanisms like the flag measure while balancing other core values. In particular, the critical issue of how to protect content while allowing its use by computers and on digital networks, in the new ways that consumers will demand in the digital age, remains unresolved.

[1] See FCC Report and Order and Further Notice of Proposed Rulemaking, MB Docket No. 02-230, In The Matter of Digital Broadcast Content Protection, released November 4, 2003. (Hereinafter cited as FCC Report and Order.)

This report is designed to provide a primer on the broadcast flag scheme, from a consumer and Internet user perspective. Among the key questions we seek to answer are:

- What is the broadcast flag?
- What did the FCC decide in its flag ruling?
- What are the major arguments for and against the flag?
- What steps should be taken by policymakers as they implement the broadcast flag regulations and consider the issues left unresolved by the FCC's initial decision?

The first half of this paper is largely descriptive in nature, providing a detailed look at the flag approach to broadcast television content protection and the arguments about it. The second half is more analytical, assessing those arguments, considering how the FCC responded to them, and providing CDT's own suggestions for addressing concerns about the flag's implementation.

Major findings of this report include:

- Protecting copyright in the digital age is important for both consumers and content owners; failing to protect broadcast content can have major implications for the availability of high-quality digital broadcast programs; and genuine fears have been raised about unauthorized redistribution of unprotected digital TV.
- The broadcast flag approach creates many legitimate concerns for television viewers, Internet users, and industry groups. The flag approach has the potential to restrict reasonable uses of content by viewers, hinder innovation, and impose costs that outweigh the benefits of the limited copy protection provided by this approach.
- The ruling recently handed down by the FCC includes some important, consumer friendly modifications to earlier proposals, but the Commission put off until its follow-on proceeding consideration of many of most important issues.
- Appropriate resolution of issues that the FCC has deferred to its further rulemaking could help address many of the outstanding concerns with the broadcast flag, particularly if the FCC creates more focused objective, functional standards for what devices and uses will be permitted by the flag regulations, and if the FCC ensures that the final process for certifying permitted technologies is open and publicly-accountable.
- Even if these issues are addressed, the flag approach will still pose unresolved concerns regarding technical regulation of computers and the Internet by the government, the impact of regulations on innovation and future consumer uses, and the definition of "fair use" and other copyright doctrines in the digital age. The flag system also leaves unresolved other serious copy protection problems for television content.
- Regardless of the future of the flag regulation in the follow-on FCC proceeding, and potential proceedings in the courts and Congress, the combination of enforcement of

existing copyright laws, introduction of new economic models and digital delivery mechanisms, and continued consumer education holds out great promise to have a broad, long-term impact on online copyright infringement.

We look forward to working with policymakers and interested parties to improve the broadcast flag system that has now been put forward by the FCC. We urgently call for an open-minded, forward-looking dialogue to seek balanced responses to the immediate challenges raised by the broadcast flag and to the broader concerns of innovation, content protection, and the user-empowerment potential of the Internet triggered by this rulemaking. The polarization of the current debate threatens these important values and our ability to deal with the piracy problem.

2. THE BROADCAST FLAG APPROACH

The mechanism referred to as "the broadcast flag" is actually composed of two parts: a simple technical method for marking digital television programs for copy protection ("the flag mark"), and FCC regulations for devices that will handle "flagged" video programs ("the flag regulations"). The flag mark, a small amount of data added to the television signal, is non-controversial. The key to the flag concept, and the controversial element, are the recently-adopted regulations requiring that DTV receivers and devices that receive content from them—such as TV sets, computers, DVD recorders, and TiVo-like digital video recorders—be built to protect DTV content marked by the flag. In this paper, we speak of the "broadcast flag approach" or "the broadcast flag system" as the combination of the marking mechanism and the regulations that require protection of marked content.

This section provides a detailed description of the broadcast flag approach. Sections 3 and 4 of the report summarize the arguments for and against the flag proposal, and set forth CDT's analysis of those arguments and suggestions for policymakers in the wake of the FCC's decision.

2.1. Introduction to the Broadcast Flag: The Rationale for the Flag

The digital world, for all its immense benefits to the creation and distribution of content, poses unique threats to copyrighted content. In the digital world, one "bit" looks much like another, whether it is part of an unprotected file or a copyrighted movie, song, or computer program. Digital content can be easily copied without any degradation over innumerable generations of copies. And with the advent of the Internet and other networks, copies—particularly of small files—can be more easily transmitted across neighborhoods and around the world.

Major content industries have watched with trepidation as computing, the Internet, and peer-to-peer file sharing systems have led to increased unauthorized copying of music, videos, software, games, and other valuable copyrighted works. The widespread piracy of copyrighted music by millions of users of file-sharing networks like Kazaa, Morpheus, or the now defunct Napster is viewed as an instructive lesson by those in the video content business. The music industry attributes major losses in revenue to widespread file sharing. While there is some debate about the extent of loss due to file sharing and the appropriate solutions for addressing the issue, it is clear that losses have been suffered and that many people online now routinely violate US copyright laws. And it is beyond question that the video content industry is very worried about the effect of the digital age on its ability to control redistribution of its works.

The threat of digital redistribution is particularly acute for movie studios and other video content producers because their business models are highly dependent on "repurposing" programming. The current movie studio business model is based on studios' ability to obtain revenue from multiple distribution windows. Licensing and distribution agreements for each stage in the life of video content—domestic and international box office, airline performance, pay-per-view, rental, home sale, satellite, premium and basic cable, and over-the-air broadcast—are critical revenue streams. Leakage from one distribution window—through

substantial unauthorized redistribution of content—could substantially diminish the value of a film or TV series.[2]

Movie and TV studios are anxious to avoid the experience of the music industry, and have expressed at least two different goals for copy protection of video:

- *Preventing one "perfect copy"* - Some studios have argued that copy protection approaches need to prevent all unauthorized leakage of digital copies in unprotected forms, because if one "perfect copy" is available online it can easily be copied and redistributed to millions through the Internet. However, many acknowledge that it will be very difficult (if not impossible) to prevent some leakage of copies.[3]

- *Creating a "speed bump"* - Others in the content industry suggest a more modest objective for video protection systems: to prevent easy widespread copying by regular consumers. They are looking for a mechanism that makes it difficult for normal consumers to engage in significant piracy—a "speed bump" approach.

As will be described below, the second of these goals is much more achievable than the first.

The triggering event for the broadcast flag discussion is America's move toward digital television ("DTV"), a transition that is supposed to occur by 2006. There is great pressure to speed this transition—in part because of the billions of dollars of analog TV spectrum it will free for other uses. However, movie studios and other video producers are concerned that people will at some point be able to share unprotected video content with the same ease that they now share unencrypted music files, and that widespread online piracy will be the result. These content providers view unprotected DTV broadcasts as an important source of unauthorized distribution and, in the absence of a copy protection scheme, some have asserted that they will not permit high quality programming to be broadcast digitally.[4] Without such programming, the fear is that consumers will not buy DTV sets—which will delay the DTV transition.[5]

---

[2] See, e.g., Joint Comments of the Motion Picture Association of America, et al., to the Federal Communications Commission, in the matter of Digital Broadcast Copy Protection, (December 2002), p. 8-10. (Hereinafter cited as MPAA Joint Comments.)

[3] For the foreseeable future, it will not be possible to stop copies (i) made from unprotected analog television outputs, (ii) made by sophisticated attackers who circumvent protections, (iii) made by those who place a camcorder in front of a television, or (iv) that come from within the studios themselves. It is well understood among technical experts that these "holes" in copy protection schemes exist and will continue to exist for many years. *See, e.g.,* Testimony of Ed Felten before the Senate Commerce Committee (September 2003); Simon Byers, Lorrie Cranor et al., Analysis of Security Vulnerabilities in the Movie Production and Distribution Process (2003). Efforts are being made to address some of these holes; for example, a subgroup of the Copy Protection Technical Working Group (CPTWG) is discussing technical approaches to analog redistribution.

[4] Viacom has withdrawn from its well-publicized assertion, and it appears that much high quality programming is already being broadcast digitally, even in the absence of a mandated copy protection system. But the threat remains.

[5] A finding that the digital transition has occurred in a particular area (and that therefore broadcasters in that area have to give back their analog channels) is dependent on penetration of DTV devices.

There is already evidence that movies and TV programs are being traded online, albeit in the case of television most commonly as digitized versions of analog broadcasts. However, a principal difference between music piracy and the threats to video is the enormous bandwidth required to download a digitized movie, even in lower-quality forms. For example, a typical MP3 music file is around 4 MB. In comparison, a VCR quality hour of standard (analog) TV compressed using current technology is about 600 MB. Ninety minutes of video on a DVD take up approximately 3 GB (i.e. 3000 MB), and an hour of high definition digital television (HDTV) is about 8.5 GB, or 2000 times larger than a typical song file.[6]

To put these numbers in perspective: while music files can, under ideal conditions, be downloaded in a minute or less, a VCR-quality hour of standard (analog) TV would require on the order of one to four hours to download over a typical home broadband connection, even assuming optimal conditions; an hour of HDTV would take in the range of 14 hours to download. As those familiar with efforts to improve broadband deployment in the US can attest, affordable access to sufficient bandwidth in the "last mile" to make downloading videos convenient is still years away for most American homes.[7]

Nevertheless, we may reasonably predict that over time improved compression and high-speed networking will make it possible to download video at ever-quicker speeds. Many people have access to faster networks already, particularly at work or school, and those numbers are growing. Though most agree that the threat of widespread copying is several years away, studios are planning ahead. Given that it can take years to implement changes to television standards, consumer electronics products, and computers, it is understandable that content producers are eager to address the video piracy problem as quickly as possible.

In the context of this prospective threat and the urgency of the DTV transition, and even though most parties agree that it does not offer perfect protection for DTV content, major content providers and others have proposed the broadcast flag as a way to provide some measure of protection for DTV content from easy redistribution (the "speed bump" approach).

---

[6] *See, e.g.,* "The Broadcast Flag and the DTV Transition," *Public Knowledge*, available at <http://www.publicknowledge.org/reading-room/documents/policy/broadcast-flag-2-pager.html>, "How Does a DVD Work," *HowStuffWorks.com*, available at <http://entertainment.howstuffworks.com/question61.htm>.

[7] Although most parties generally agree that download times for digital video files are currently prohibitively large for most end users, estimates vary substantially regarding both the exact amount of time typically required to download video content and the amount of time required before download times decrease enough for downloads of video content to become routine. Our own estimates for download times are based on current downloads speeds for cable and DSL, which generally range (at optimal speeds) from 128 kbps to 1.5 megabits/second (although some providers are already experimenting with 3 Mbps services). Regarding the penetration of high bandwidth access, even though cable and DSL technologies have been around for some time, as of May 2003, Nielsen//NetRatings reports that only 13% of Americans connect to the Internet via broadband and narrowband users still outnumber broadband users 2 to 1, although they estimate that over the last year broadband access has grown by 50% (see Nielsen//NetRatings Press Release, "Nearly 40 Million Internet Users Connect via Broadband," June 17, 2003.). Widespread penetration of higher bandwidth broadband technologies is expected to be substantially slower. Improved compression technologies also promise to decrease download times, but adoption remains some time off.

2.2. Origins of the Broadcast Flag Proposal: The BPDG Report

The parties trying to craft a solution to DTV piracy concerns faced several hurdles. The most logical protection measure—scrambling of DTV content "at the source" (encryption by the transmitter, instead of by the machine receiving the signal) as is found in satellite or cable broadcasts—would mean that existing digital television receivers would not be able to receive DTV content without a special added device, imposing a cost on several hundred thousand early-adopter owners of DTV sets.[8] Some believed broadcast encryption was also politically unworkable given a long US tradition of public access to broadcast television.

Broader approaches to addressing video copying were also disfavored. For example, an early legislative proposal to mark all digital copyrighted works and require all devices that handle content to check for the marks and protect the works would have created protections for a broad class of video content.[9] But it met substantial opposition from computer and consumer electronics makers because there was no readily apparent engineering solution available to implement such marks (particularly in computers), any such solutions were expected to be very costly and create consumer concerns, and many feared such marks could be easily defeated.

Content providers, together with a technology consortium that had developed promising copy-prevention technologies (the 5C group),[10] urged that the DTV protection issue be taken up at the Copy Protection Technical Working Group (CPTWG), a group including representatives of the entertainment, consumer electronics, and information technology industries as well as several consumer groups at times. A sub-group, the Broadcast Protection Discussion Group (BPDG), was charged with evaluating technical approaches to protecting digital television broadcasts.[11]

The result of the BPDG's work was the report of the Co-Chairs of the BPDG, published in June 2002.[12] It is fair to say that the BPDG process and the co-chairs' report itself were controversial, even among many BPDG participants. In mid-June 2002, the BPDG gave its

[8] The Consumer Electronics Association reported that about 700,000 receivers had been manufactured through June 30, 2003. Because of reception problems, it is estimated that less than half that many are actually in consumers' hands for broadcast reception. Proponents of broadcast encryption note that, while high in absolute terms, these numbers are low compared with, for example, the installed base of DVD players (of which about 40 million are today in consumers' homes) whose utility could be affected by DTV copy protections. See below.

[9] Consumer Broadband and Digital Television Promotion Act, S. 2048, introduced March 2002.

[10] The "5C" consortium is made up of Hitachi Ltd., Intel Corporation, Matushita Electric Industrial Co. Ltd., Sony Corporation, and Toshiba Corporation. 5C has developed the Digital Transmission Content Protection System, or DTCP, which offers secure electrical transmission of compressed content over particular digital interconnections. DTLA is the licensing authority joint venture founded by the 5C companies, which administers the licensing of DTCP.

[11] The CPTWG and BPDG are informal discussion groups whose meetings are open to any interested party (except members of the press). On the order of 50-100 different organizations appear to participate regularly. In the past few years as many as five or six public interest consumer groups have participated, though only one (the Electronic Frontier Foundation) was heavily active in the BPDG deliberations.

[12] Final Report of the Co-Chairs of the Broadcast Flag Protection Discussion Subgroup (BPDG) to the Copy Protection Technical Working Group (CPTWG) (June 3, 2002).

report to Representative Billy Tauzin (R-Louisiana), Chairman of the House Commerce Committee, who had urged the companies to undertake the initiative. There had been indications that Rep. Tauzin would propose legislation concerning the broadcast flag.

The BPDG report evaluated the creation of a flag signaling protected content and a set of "robustness and compliance" rules, which proponents argued would ensure that marked content was appropriately protected by the machines receiving it. The flag system contemplated that all devices capable of demodulating DTV television signals would protect DTV content until it could be checked for the flag. Content recognized as "flagged" would have to be protected within such devices and could not, in most instances, be recorded or output in a digital form other than by an authorized recording or output technology. Those demodulating devices would then be able to send marked content to other secure "downstream devices" that also protected the digital content, subject to robustness and compliance requirements designed to ensure that the copy protection would not be circumvented.

2.3. Overview of the Flag Rule

The BPDG report left many major questions unanswered: What usage rules would be established? What was the scope of the protection? What copy protection technologies would be approved, and how would future technologies be added to the list? These questions, and whether the flag system itself was appropriate, became the basis for the FCC's rule-making effort launched in the fall of 2002.[13]

The FCC's Notice of Proposed Rule-making did not propose a specific rule. The only complete proposal for a broadcast flag was the one put forth by the Motion Picture Association of America (MPAA) and others and supported by the Digital Transmission Licensing Administrator, LLC (DTLA) (the "MPAA proposal").[14] This proposed rule set out in detail how DTV broadcasts would be flagged, how devices would be required to handle flagged content, and what technologies would be approved for the handling of protected content.

The proposed flag mark has already been added to the standards for DTV by the digital television standards body.[15] It consists of a small field in the digital broadcast signal that is not part of the video or audio data and does not interfere with the picture or the sound. The mark contains very little information. It is either on or off, indicating when "technological control of consumer redistribution is signaled." The standard cannot by itself create any obligation for machines to respond to the flag. The flag mark itself, therefore, is not a subject of great controversy.

---

[13] See FCC Notice of Proposed Rulemaking, MB Docket No. 02-230, In The Matter of Digital Broadcast Copy Protection, released August 9, 2002. (Hereinafter "FCC Notice of Proposed Rulemaking.")

[14] DTLA is the licensing authority joint venture founded by the 5C companies. A proposed regulation was submitted to the FCC in December 2002 by the MPAA and 5C, and revised in reply comments filed by the MPAA. For purposes of this paper, we refer to the original proposed regulation as amended by the MPAA Reply Comments as the "MPAA proposal." See Joint Reply Comments of the Motion Picture Association of America, et al., to the Federal Communications Commission, in the matter of Digital Broadcast Copy Protection, (February 2003).

[15] The flag mark is technically known as the "Redistribution Control Descriptor." See ATSC Standard A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable, Rev. B (18 March 2003), p.78.

The bulk of the debate at the FCC has dealt with how flagged content will be handled by consumer devices. The rule adopted by the FCC in November of 2003 requires that, after July 2005, any new device capable of demodulating DTV content must–

1. check for the presence of the flag;
2. encrypt any flagged content using "authorized technologies;"
3. allow digital recordings of flagged content using only authorized technologies; and
4. allow digital transmission of flagged content only via secured digital outputs using authorized technology to other "compliant" devices (authorized devices that are appropriately secure and themselves ensure that protected content can only be handled as required by the authorized technology that delivered the content).

Collectively, these requirements are referred to in the FCC rule as Compliance Requirements.[16] An overview follows.

Checking for presence of the flag. The FCC rule requires that machines that receive digital television broadcasts be required to react in one of three ways:

1. If the content has been checked for the flag, and the flag is present, it must be treated as "marked content." "Marked content" is subject to the rules set by the flag process (discussed below), and may not be digitally transmitted over wires to insufficiently secure (noncompliant) devices.
2. If the content has been checked for the flag, and the flag is not present, the content must be treated as "unmarked." No rules need be followed, and the unmarked content can be copied and distributed freely.
3. If the content has not been checked for presence of the flag, it must be treated as "unscreened content." Such content must not be transmitted digitally over wires to devices that are insufficiently secure.

Use of approved technologies. The FCC rule requires that all new equipment capable of demodulating a DTV signal must build-in approved protection technologies that prevent certain unauthorized copying or redistribution.[17] These devices include future digital televisions and set-top boxes, but also include computers or other future hardware or software capable of demodulating a DTV broadcast. Approved technologies will use encryption and other techniques to ensure that the standards for use and distribution are obeyed.

Under the FCC rule, only digital output to "Authorized Digital Output Technology" (Authorized Technology) is permitted for marked programs.

Equipment using Authorized Technology must agree to the license requirements associated with these technologies. Such licenses will include rules about compliance ("how may consumers use a device to handle marked content?") and robustness ("how is the device

[16] See FCC Report and Order, p. 21-22.

[17] The FCC has indicated that protection technologies will be designed to prohibit indiscriminate redistribution on the Internet; as noted below, the language of the proposed rule is not definitive as to what behaviors will actually be allowed or prohibited by approved protection technologies.

designed? how resistant is the device to tampering?"), and could also include patent licensing, interoperability, or other commercial terms.

Regulation of "downstream devices." In order to protect flagged content once it has been recognized, any device that handles the content would also need to respect and adhere to the protections. The FCC rule does not directly regulate all equipment that receives flagged content through digital interfaces. Rather, such downstream devices are regulated indirectly since Authorized Technologies will typically require that all such devices be "compliant" by themselves incorporating Authorized Technology and adhering to license requirements. Affected devices include digital video recorders and DVD burners, as well as any other device that could receive protected content—like a computer, a handheld device, or a 3G mobile phone.[18]

Robustness Requirements: In order to ensure that it is difficult to circumvent the protections mandated by the Compliance Requirements by hacking into devices, the FCC adopted a set of "Robustness Requirements" for regulated devices. These require that products meet a specified level of secure design and construction, so that the Compliance Requirements cannot be easily circumvented. The standard chosen by the FCC—that the flag rules cannot be defeated "merely by an ordinary user using generally available tools or equipment"[19]—was welcomed by consumers and device makers who viewed the higher standard of care that had been proposed by flag supporters as too costly to implement and offering little ultimate benefit.

In order to assess how the flag will protect DTV content—and in order to understand its impact on consumers and device makers—two questions need further exploration: What copy protection technologies will be approved to handle flagged content? And what uses of that content will be permitted?

2.4 What Technologies will be Permitted?

The linchpin of the flag regulation is the mandated use of copy protection technologies that handle protected DTV programs. The list of Authorized Technologies is therefore critical to both consumer electronics and IT companies (who want to sell products that will need to include Authorized Technology) and consumers and computer users (who will need to use these technologies if they want to view and use DTV broadcasts).

What technologies will be authorized? The authorization process originally proposed by MPAA rule included two avenues for approving technologies: the "industry acceptance" process, and the "equally effective as" process:

- *Industry acceptance.* The MPAA approach proposed that a technology could be authorized if it was used or approved by three major studios; used or approved by three major television broadcast groups; or licensed by ten major device manufacturers and used or approved by two major studios.

[18] It should be noted that the FCC rule does not place limits on analog copying or analog outputs, just on digital copying and digital outputs. This will permit the many existing televisions (including HDTV-capable sets) and VCRs, with their analog interfaces, to continue to work with flagged content and devices that handle it. (As noted below, it also permits conversion of such content back into unprotected digital form.)

[19] FCC Report and Order, Appendix B, p. 43.

- *Equally effective.* The proposal also suggested that a technology could be authorized if it was found to be "at least as effective at protecting [content] against unauthorized redistribution (including unauthorized Internet redistribution) as," any already authorized technology, taking its licensing terms and other factors into account.

Realizing the difficulty of the approval issue and responding to criticisms that this process put too much control in the hands of studios and provided no clear, objective standards for evaluating technologies, the FCC put off final determination of the approval process to its follow-on proceeding. In its "Further Notice of Proposed Rulemaking" the Commission seeks comment on "standards and procedures…adopted for the approval of new content protection and recording technologies."[20]

In the meantime, the FCC has created a process for "Interim Approval of Authorized Digital Output Protection."[21] The process has three phases:

- *Application:* Under the process, proponents of particular digital output protection technologies have thirty days, starting from the issue of a public notice to be issued by the FCC, to make a case to the FCC that their technology should be approved. Documentation must include a description of how the technology works, a detailed analysis of the level of protection afforded by the technology, the record of approval or adoption of the technology by industry players, and a copy of the licensing terms for the technology.
- *Challenge and Response:* Following the close of this thirty day period, all parties will have twenty days to file oppositions to the approval of submitted technologies. Challenged technologies will have ten days following the close of the twenty-day opposition period to respond.
- *Determination:* The timetable for a decision on approval of a technology is different depending on whether or not the technology has been challenged.
    - For technologies to which no objection is issued by the end of the challenge and response process, the Commission will "expeditiously issue a determination"[22] indicating whether the technology is approved.
    - For technologies that are challenged, the Commission must undertake a full review of the technologies' merits (utilizing the criteria described below) before issuing a determination on the approval of those technologies. No time frame is given for this process.

In the case of unchallenged technologies, where the Commission undertakes an "expeditious" review of the certification, the specific criteria that will be used in this review are not specified in the ruling.

In the case of challenged technologies, where a full review is called for, the ruling provides a non-exhaustive list of factors the Commission may (though is not required to) consider.

---

[20] FCC Report and Order, p. 29.

[21] FCC Report and Order, Appendix B, p. 43.

[22] FCC Report and Order, Appendix B, p. 44.

These general guidelines include "technological factors," "applicable licensing terms" and "the extent to which the [technology] accommodates consumers' use and enjoyment" of broadcast content. In addition, the FCC may consider "any other relevant factors the Commission determines warrant consideration."[23]

Applications for approval of technologies under the interim process can also be submitted after the initial thirty-day window for submissions has passed. In this case, the same process applies except that the twenty-day challenge period starts immediately from the public notice of the filing of the application.

The FCC's ruling also provides for revocation of authorization in cases where a protection technology has been compromised. Parties may petition for revocation of approval under a standing FCC procedure.[24] The ruling does not specify what criteria the FCC will use in deciding whether a technology has been sufficiently compromised to warrant revoking its authorization.

What will the list of Authorized Technologies look like at the beginning? The BPDG Co-Chairs' final report suggested that a set of four complementary technologies—popularly referred to as the "5C suite"—be considered suitable for immediate approval. The MPAA proposal before the FCC indicated that the technologies in the 5C suite "have already gained sufficient industry acceptance to qualify as authorized technologies."[25] The FCC did not list the 5C suite or any other technology as "pre-approved" in its rule, but it seems virtually certain that the 5C suite will be submitted for certification as Approved Technologies as soon as the FCC opens its interim approval process.

The four technologies currently in the 5C suite are:

- DTCP, which offers secure transmission of compressed content over electrical connections, like those to a computer or an on-board DVD player in a mini-van;
- CPRM, which offers secure storage of compressed content, say for authorized copying of a program onto a CD;
- HDCP, which offers secure transmission of uncompressed protected content over an electrical interconnection (DVI), used for displays; and
- D-VHS, which offers secure storage of uncompressed protected content.

These four technologies all do different things, and each occupies a different market niche. Together they provide a reasonably comprehensive set of technologies for protecting digital video content in the home environment, though they are limited in terms of use on new networks or the Internet.[26]

---

[23] FCC Report and Order, Appendix B, p. 45.

[24] FCC Report and Order, Appendix B, p. 45.

[25] MPAA et al. Joint Comments, Attachment A.

[26] Today, none of these technologies allow transmission over the Internet of protected content. Until recently, none allowed transmission of flagged content over wireless networks. In late September 2003, the DTLA announced that it had adopted DTCP for WiFi devices. The resulting technology will be known as DTCP-IP. It is not clear whether studios are prepared to support such networking using 5C technology.

Significantly, the DTLA license for DTCP does not allow digital outputs of content to non-5C devices.[27] This means that once a consumer builds a home network based on DTCP, the network will form a closed circle—no devices can be added to that network unless they also are part of the 5C world.

It is not known whether any other competing technologies—such as Microsoft's Windows Media Player system or the protection system employed in TiVo personal video recorders—will initially be submitted for approval in the interim process.

2.5. What Uses will be Permitted? The 5C Encoding Rules Example.

What uses of flagged content will be allowed? Will users be allowed to freely copy marked programs, view them on multiple devices, or email them? The broadcast flag rules do not clearly indicate what kinds of uses will be permitted in practice for flagged content. Since nobody is sure what technologies will be approved or even which will be submitted for consideration—except 5C—the 5C rules for using content are especially instructive.

The encoding rules for 5C ("what may be done with flagged content protected by 5C?") are determined by the 5C licensing agreement. 5C allows digital use of DTV content in accordance with four possible settings:

1. *copy freely* - encryption/decryption not required at all and 5C not applied (for unprotected content like news, public affairs programs, e.g.);
2. *EPN (encryption plus non-assertion)* - This is the setting that will be applied to flagged DTV content. It requires that all copies have to be encrypted—and can only be read on another 5C-compliant device—but allows users to make as many copies as they want on 5C devices;[28]
3. *copy one generation* - for subscription television. Content can be copied once but cannot be copied further—you can make a copy but cannot make a copy of the copy;[29] and
4. *copy never* - for pay-per-view television. Content cannot be copied. For personal video recorders, "copy never" is subject to an exception—this rule can be set to

[27] The DTCP license does permit "constrained" (down-resolutioned) digital output over a DVI interface to computer products manufactured before 2005, but many do not view this exception as broad enough to serve public interest purposes. Data traveling over a DVI interface is uncompressed, and therefore extremely large and unwieldy, and restrictions on image quality are likely to diminish consumers' enjoyment and use of lawfully acquired content. The license also permits the use of technologies other than CPRM or D-VHS for the making of up to two first-generation copies, provided that the copy cannot be played on any device other than the device making the copy. This, too, is a narrow exception that may not serve consumers' interest in intercompatibility.

[28] 5C creates a secure channel to transmit marked content to another device, after "checking" (authenticating) whether the second device has 5C installed. Because 5C does not allow its authentication/encryption "handshake" sequence to take place over an Internet connection, this setting bars emailing flagged content or opening a flagged file to the public Internet. Thus, this setting also bars emailing excerpts of flagged content. 5C was designed to protect content delivered to the home network, not to provide for secure Internet transmission.

[29] We understand that the 1394 connection allows sending a file simultaneously to 62 different recording devices. Thus, "copy one generation" would allow a user to make 62 different simultaneous copies, but each of those copies would be marked "copy no more."

> mean “copy never but watch for a limited period of time,” with a maximum of 90 minutes of “pause” time from the time the program is downloaded.

EPN is most relevant to the flag proposal. All flagged DTV content would be treated by 5C devices as EPN, meaning that 5C devices can send it to any other 5C device—although at this point 5C devices can only be connected on certain kinds of local networks, so this does not and currently will not permit redistribution over the Internet. EPN also allows users to make as many physical copies of a program as they want, so long as they make these copies and play them back on other 5C devices that agree to obey the same rules.[30]

The 5C technologies provide an illustrative example, but the flag regulation itself has left different groups with different interpretations of what uses will ultimately be allowed by approved technologies. *The touchstone of the FCC regulation is this stated goal: to "prevent the indiscriminate redistribution of [digital broadcast] content over the Internet or through similar means."* The FCC specifies that this goal is not intended to interfere with consumer copying or use of content within the home or “similar personal environment,” nor is it intended to “foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution.” In addition, the FCC’s ruling indicates that the Commission will evaluate, in its follow-on proceeding, whether it makes sense to try to define a “personal digital network environment,” within which redistribution of content would be permitted by the flag regulations.[31]

This stated goal does not clearly answer the question of what uses will be permitted by the flag regulation. To start with, the Interim Approval process now in effect under the regulation does not incorporate the "indiscriminate redistribution" language—in fact those words do not appear anywhere within the final rules adopted by the Commission. As noted above, the final rule itself in fact provides no criteria for approval of uses beyond a list of factors that the FCC may consider in reviewing the merits of a request for certification of an authorized technology. The critical question of what uses and technologies will be permitted is saved for the follow-on rulemaking.

For their part, some studios have indicated a relatively permissive view of what actions would be permitted under future sets of encoding rules in connection with new Authorized Technologies. They indicate that technologies could be approved that allow unlimited use of programming in the home environment, and a large amount of physical copying as well—so long as secure technologies are used that do not permit widespread Internet distribution. As MPAA General Counsel Fritz Attaway indicated in Congressional testimony in Spring 2003:

> “The broadcast flag does not prevent copying at all, as I stated earlier. With today’s technology, it would prevent [a] student from e-mailing [a] project [including marked video content] because a secure system does not yet exist for e-mailing. But as soon as that technology is developed, and I believe it will be, then that would be made possible, as well. The only thing that the flag is

[30] The creators of 5C indicate that these categories represent ceilings, not floors, for particular kinds of programming. If, for example, basic cable programming was marked “copy never,” that would be a violation of the 5C license. It is not expected that these encoding rules would ever change, although it is possible that the licensors of 5C technology could change them.

[31] FCC Report and Order, p. 6.

> designed to do is to prevent the mass redistribution of television programs on wide-area networks like the Internet."[32]

At the same time, consumer groups have raised concerns that the flag regulations together with the licensing terms for Approved Technologies may limit many uses in practice, especially innovative new uses. For example, they worry that secure technologies may never be approved that would allow people to securely email a program or an excerpt of a show. They also wonder whether a more restrictive future version of 5C, or some more restrictive replacement for 5C, could become a dominant and limiting technology.

At this time, under the current proposal, there is no way to know exactly what uses will ultimately be permitted of flagged content in practice. This state of play is likely to confuse many who are trying to evaluate the flag proposal.

[32] Testimony of Frtiz Attaway before the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property (March 6, 2003).

3. THE BROADCAST FLAG POLICY DEBATE

The broadcast flag has become a topic of extensive debate in Washington. The FCC Notice of Proposed Rule-Making in connection with the flag proposal prompted over 5000 comments. Most were filed by individuals concerned about the flag proposal's impact.

Supporters in the content industry have touted the flag approach's narrow focus, and have stressed to the FCC the growing need for protection given the planned transition to DTV. Consumer groups have raised questions about risks to reasonable uses of content posed by the flag regulations, as well as questions about their effectiveness and their impact on future consumer products. Many information technology and consumer electronics companies have raised concerns about the impact of the proposal on innovation, the costs of content protection, whether reasonable uses of devices will be permitted, and whether the FCC will face increasing pressure to regulate further given the limited scope of the proposal's protections.

The policy debate that may have the most immediate impact on the flag regulations, however, is not about the substance of the rule, but rather the manner in which it was enacted. Several groups have argued that the FCC does not have the authority to mandate the flag scheme, and as of December 2003 were considering legal challenges on these grounds.

3.1. Assessing the Flag: Themes

Four themes have emerged in our interviews with stakeholders:

Content Protection. The producers and distributors of digital television broadcasts fear uncontrolled, massive online redistribution of their content if it is broadcast digitally without protection. Because content producers may have greater incentives to distribute high-quality programming by broadcast if it is protected, significant consumer benefits may flow from some form of protection.

Future Innovation. Many information technology (IT) companies, consumer groups, and some consumer electronics (CE) companies have expressed great concern that a flag regulation will damage competition and innovation. In particular, they worry about establishing gatekeepers over future product development and creating a precedent that stimulates further and broader regulation. They have argued that functional and objective standards for Approved Technologies are better for the marketplace and for consumers.

Reasonable Uses of Content. Consumers want to use content in reasonable ways, including time-shifting (watching a program at a different time), space-shifting (watching a program in a different place), and other, innovative forms of reasonable copying and sharing. Many are also concerned that certain "fair uses" rooted in copyright law and the First Amendment are threatened by the flag approach.

Public Interest Values. Many consumer groups want to ensure that flag regulations protect the lawful free flow of information over the Internet and other important free speech values. They have argued that news, public affairs, and other programming important for public discourse should not be flagged, and that flag technologies should

not require the collection of private information in order for people to have access to flagged content.

No group we spoke with disagreed with these goals in general. However, in assessing the flag, different groups have reached different conclusions based on how they reconcile tensions among these competing aims. The following sections summarize the arguments we have heard.

3.2. Need for Content Protection

We heard broad agreement that massive online redistribution of broadcast video should be avoided, and that copyright protection of DTV has substantial public benefits. We also heard agreement that both licenses and technical protection measures (at some level) will be used to protect content in the future. While some parties view technological content protection solutions like the broadcast flag system as, at best, a necessary evil, many agree that content protection technologies can provide important benefits for consumers as well as for content owners.[33] We encountered deep disagreement, however, as to the role of the Federal government in requiring companies to adopt such protections through regulations like the broadcast flag rules.

The MPAA Consortium has stated that implementation of the broadcast flag scheme is essential to protect the continued viability of free over-the-air broadcasting, and that, without the flag, free broadcasting will be at a competitive disadvantage. They reiterate that broadcast program suppliers rely on after-markets like syndication, foreign distribution, and home video sales, because TV license fees alone do not cover the cost of production. They point out that cable and satellite services, because they operate through conditional access systems, can offer program suppliers technological protections against Internet redistribution of their programs, and broadcasters cannot. They suggest that the flag is needed in order to provide a level playing field among cable, satellite, and broadcast television, and they argue that some program distributors will not license high-value HDTV programs to free broadcasters in the absence of a flag scheme.

Others have argued, however, that protection of aftermarkets for digital broadcast television should not necessarily dictate that every device touching DTV content (including general purpose computers) be redesigned to incorporate approved technologies that prohibit not only all online redistribution but also all copying and playing by noncompliant devices. Moreover, there is considerable concern that government regulation should not be used to protect existing market models, which are clearly evolving in the digital age just as they have in the face of technologies like the player piano, the radio, the television, and the VCR. Such critics also point out that there probably never has been a level playing field between cable and satellite, on the one hand, and broadcast, on the other.[34] These critics have noted that

[33] For example, defenders of technological approaches to content protection (also know as digital rights management or DRM systems) note that such technologies could allow content providers to offer diverse rights packages to consumers—from low-cost, transient uses of content (like streaming a movie in real time) to higher-cost, valued-added packages (like renting a movie for a month or being able to manipulate it). The digital world has the potential to give rise to exciting new business models that will be attractive to consumers.

[34] These commentators note that cable and satellite distributors condition access to their programming on the payment of fees—fees they share with creators of content, making their channel more desirable for such creators and distributors.

Congress and the FCC have received no guarantee either that program distributors would not license HDTV programs to broadcasters in the absence of a flag scheme or that such distributors will license *more* programs to broadcasters when the flag is mandated.[35]

In its ruling, the FCC largely accepted the MPAA's argument for the need for the flag, writing that "the potential threat of mass indiscriminate redistribution will deter content owners from making high value digital content available through broadcasting outlets absent some content protection mechanism."[36]

Several of the flag scheme's critics have suggested "encryption at the source" as an alternative to the broadcast flag. Under such a solution, broadcasters would encrypt their broadcasts rather than broadcasting "in the clear" and having encryption take place at the receiver level. This is the content protection approach employed in cable and satellite television systems.

Although this solution may be more technically elegant, and provide better protection to content, many view it as politically infeasible because of the US tradition of free over the air broadcast. Additionally, encryption would leave those television receivers in consumer hands today unable to receive DTV broadcast content, and consumers would have to buy converters.[37] Estimates for the cost of these converters range widely, but they would probably cost on the order of $100 each for several hundred thousand users. In its ruling, the FCC cited concerns over "the implementation costs and delays" associated with a solution based on encryption at the source as its reason for preferring the flag approach.[38]

Critics of the flag have also noted in some detail how limited the flag's protections may turn out to be. Broadcast in the clear, DTV signals will remain susceptible to interception by demodulators that are not compliant with the law but may be easy to build or obtain. Analog outputs in flag-compliant devices—critical to ensuring that tens of millions of analog TVs, VCRs, and DVD recorders continue to function—will permit easy redigitization of DTV broadcasts. Hundreds of thousands of existing DTV receivers, manufactured before the flag rule takes effect, will continue to allow digital output of DTV programs. Other sources of video content will remain, such as theft by studio employees and contractors or even recordings of a program or movie made with a video camera. In response, some proponents note that the flag is part of a long term strategy to protect digital copyrights, that it is only one step in limiting sources of video content online, and that the flag has a more limited goal of making easy, widespread unauthorized redistribution of DTV broadcasts more difficult for the average unsophisticated consumer.

Having listened carefully to all of these points of view, we believe that providers of broadcast digital television have articulated a real problem that they are making a serious effort to address. Content provider concerns about the long-term risk of widespread online copying

---

[35] Many consumer groups are not convinced that the studios' arguments in support of using the broadcast flag proposal to solve the problem of massive online redistribution are compelling. Nor are all convinced that the studios have stated a real problem, in large part due to "last mile" bandwidth issues.

[36] FCC Report and Order, p. 3

[37] We also heard that since high definition digital television (HDTV) is being transmitted in compressed form, it requires converters and decoders in order to be viewed on standard digital televisions anyway.

[38] FCC Report and Order, p 12.

of DTV content have merit, and it is reasonable to seek a solution with all deliberate speed rather than waiting until it is too late. At the same time, it must be recognized that the broadcast flag regulations will not make unauthorized distribution impossible or prevent the appearance of "perfect" digital copies of DTV content online. Rather, the major rationale for the broadcast flag is as a "speed bump," whose effect will be merely to make it harder for average users to engage in large-scale unauthorized redistribution of digital broadcast television content outside the home network. The FCC recognized this limited scope for the flag. We agree that implementation of the broadcast flag would probably help make widespread online redistribution of DTV more difficult for the average consumer—though by no means impossible.

3.3. Innovation Concerns

Many members of the IT and CE industries (as well as consumers) are concerned about competition and innovation. In particular, many companies are worried that the proposed flag regulation will establish "gatekeepers" over future product development, which are free under the proposal to apply subjective criteria in withholding approval of new products. They argue that more neutral and functional flag criteria or standards for "approved technologies" are better for the marketplace and for consumers. As noted above, the FCC has stated its intention of taking up these issues in its follow on proceeding, asking for comments on "whether objective criteria should be used to evaluate new content protection and recording technology and, if so, what specific criteria should be used."[39] IT and CE companies remain concerned about what the final rules will look like. In the meantime, the FCC has included a list of general list of factors to be considered in the interim approval process, though critics argue that these factors are vague and non-exhaustive, still leaving wide room for subjectivity in the Commission's rulings.

Many critics of the flag approach are also concerned that the flag rule is just the first in a serious of rules that will broadly chill innovation. Given the limited protections offered by the "speed bump" model of the flag, they fear that the FCC will be under increasing pressure to augment the flag system with additional control over information technology and consumer electronics devices. The Commission's ruling does not state any specific intention to adopt future rules to address, for example, the analog hole, and the Commission argues in its report that the flag approach is justified even in the absence of any such solution.[40] However, other parts of the Commission's report do strongly suggest that the Commission will seriously consider further regulations to plug the analog hole, thus validating the fears of critics.[41]

For their part, the flag's supporters have stated that in order to protect intellectual property rights they need a governmental mandate requiring all devices that touch digital broadcast

[39] FCC Report and Order, Appendix B, p. 29

[40] "We believe, however, that the benefits achieved by the creation of a flag-based system—creating a "speed bump" mechanism to prevent indiscriminate redistribution of broadcast content and ensure the continued availability of high value content to broadcast outlets—outweighs the potential vulnerabilities cited by commenters." FCC Report and Order, p. 9-10.

[41] For example, the Commission writes, "We recognize that the ARDG [(Analog Reconversion Discussion Group)] is discussing watermarking and fingerprinting among various alternative solutions to the analog hole. We encourage the further development of alternative mechanisms and technologies that could be used to protect digital broadcast content in the future." FCC Report and Order, p. 13.

content to be sufficiently "robust" (secure and nontamperable) and "compliant" (possessed of approved technology to prevent unauthorized flows of content through digital outputs). They argue that this request is merely incremental and that, in the future, virtually all TV equipment will already contain protected inputs and outputs in order to make use of protected content delivered by cable and satellite services. Therefore implementation of the flag will merely require flagged broadcast programming to be directed to these preexisting protected inputs and outputs—which in many cases will already be protected by the 5C suite of technologies.[42]

Consumers and content providers both stand to benefit from competition among multiple potential protection technologies. However, discussions of the proposed regulation almost always take it as a given that the 5C suite of technologies will be approved and it remains unclear what other technologies will be initially authorized by the Commission. Concerns have been raised that this "first-mover" advantage for 5C, coupled with the hurdle of the authorization process and the potential use of licensing terms to stifle competition and interoperability, could have unintentionally anticompetitive effects. In some regards, the FCC ruling creates the worst of both worlds with respect to this concern: it puts the flag requirements in place while deferring the question of how to create real competition between technologies to implement this requirement. The first mover advantage gained by technologies approved in the FCC's interim process may be amplified by the uncertainty surrounding the shape of the final authorization process.

Several parties are specifically concerned about the effect of implementation of Authorized Technologies on innovation with respect to the general-purpose computer. As we understand it, the 5C license would not permit transmitting flagged content to a computer through a digital connection unless the computer is "compliant"—i.e. has secure digital outputs—and meets the Commission's robustness requirements. This would require the general-purpose computer—still an open platform device—to become "untamperable" and would mean that computer makers who want their devices to participate in home networks will not be permitted to have unregulated digital outputs, a major architectural change. Computer makers will have to create different product lines if they wish to keep some digital outputs unregulated. This creates a real concern that the flag proposal will extend far beyond the devices typically thought of as processing digital TV and squarely impact the open architecture of the computer, which has been a driving force in the digital revolution.

The Commission made an attempt to answer the concerns regarding the computer in two ways. First, in its report the FCC articulated an interest in and openness to software-based protection technologies.[43] Second, the Commission attempted to structure its robustness rules to account for the general-purpose computer.[44] It did this by adopting the "ordinary

[42] Some have noted that this "incremental" argument depends in significant part on the Cable/CE Memorandum of Understanding currently being finalized by the FCC. Because the final contours of that agreement are not known, some believe it would be unwise to assume that all future devices will incorporate the 5C associated technologies. Moreover, this agreement as well as the flag regulation create concerns for the IT industry about the increasing role of federal regulation in dictating personal computer architecture. See FCC Report and Order and Further Notice of Proposed Rulemaking, CS Docket No. 97-80, In The Matter of Compatibility Between Cable Systems and Consumer Electronics Equipment, released October 9, 2003.

[43] FCC Report and Order, p. 6.

[44] FCC Report and Order, p 21.

user" standard mentioned above in place of the more restrictive "expert" level standard suggested in the MPAA's proposal. These are welcome revisions. However, some concerns still remain. For example, the Commission has put off to its follow-on proceeding the concern that the flag regulations will preclude handling of DTV content by open-source programs,[45] a potentially important roadblock with respect to innovation.

3.4. Reasonable Consumer Uses

Consumers are just beginning to learn about copying and sharing video files, and they will expect to be able to continue to do so on interoperable devices for their own private purposes. Consumers enjoy recording, storing, and viewing programs in many different places. They own a great deal of legacy equipment and will be frustrated if their machines stop working with DTV content.

The only measure in the flag rule to help ensure that approved technologies provide for reasonable consumer uses is the inclusion, as one of the general factors which the Commission may (though is not required to) consider as part of a full review of an application for Authorization, the extent to which the technology "accommodates consumers' use and enjoyment" of DTV broadcasts. Reasonable consumer uses of content include recording a program onto standard-format, non-compliant devices; time-shifting (to watch a program at a later time); space-shifting (to watch a program in a different place); excerpting; skipping over content consumers do not want to see; transferring content within a personal network and among formats; continuing to watch content on millions of legacy devices; and other as-yet-unrealized reasonable uses of content (such as, for example, securely emailing files to family members).

While many of these uses might be permitted by 5C technology (or future versions of 5C technology), critics of the flag approach fear that protection technologies that restrict more uses might become dominant, giving consumers little choice but to forego some reasonable uses in order to access DTV content. Defenders of the flag scheme argue that competition among technologies will ensure that attractive, permissive options emerge, but critics remain concerned about the prospects for a diverse, competitive market given the regulatory burdens imposed by the flag rules.

The flag's supporters have asserted that the broadcast flag will not prevent any of the activities that the typical consumer engages in today with television, including recording and copying programs. This is a welcome statement for consumers but is best understood with certain caveats. As noted, the language of the FCC rule is not clear on this point. Also, a consumer may be required to purchase new equipment to continue to enjoy these activities. For example, once a 5C-compliant device recognizes flagged content, it cannot be transmitted to (or played on, or copied by) any noncompliant legacy device. So while 5C's EPN encoding rule may allow unlimited physical copies (like DVD recordings) and even transmission within a home network (like through a WiFi network),[46] consumers will only be able to view those copies or transmissions on compliant devices.

---

[45] FCC Report and Order, p 28-29.

[46] One of the difficult questions raised in the FCC's follow-on proceeding is how to define a "personal digital network environment." See FCC Report and Order, p. 29.

For many consumers, this means they may need to substantially upgrade or replace their televisions, DVD players, computers, and other devices to handle flagged content if they wish to do many of the same things that they are able to do with broadcast content today. Consider a consumer who buys one of the increasingly popular DVD recorders, personal digital recorders (like TiVo), or other digital recorders in a few years when we expect VCRs will be increasingly less attractive and when the flag will be in place. That consumer will be able to record a favorite DTV show on her flag-compliant recorder, just as she does today, and play it back on that same recorder. But she will not be able to play that show back on any of her existing, non-compliant DVD players or computers; her compliant recordings will not operate with her existing non-compliant devices as required. The FCC acknowledged this concern in a footnote to its ruling, but dismisses it is a "single, narrow" example.[47] On the contrary, as Americans make the transition to DTV and digital recording—and the flag ruling clearly contemplates that they will—we believe there will be manifold incompatibility issues that will impact millions of consumers.[48]

The flag also raises concerns because it provides no guarantees that consumers will be able to share content—even securely—over network connections. Given the explosive growth of the Internet and wireless networks like WiFi, this approach seems destined to upset consumers. For example, consumers might expect to send excerpts of content (or entire shows) to their families via the Internet. An increasing number of homes and offices will have WiFi networks and might expect to send programming over them. The FCC has indicated that it does not wish to "foreclose use of the Internet" to securely transmit flagged programs or to otherwise restrict uses other than "indiscriminate redistribution" of content online. However, little guarantee is offered that the list of Authorized Technologies will include technology that makes such reasonable redistribution by consumers possible.

Some are also concerned about future, innovative uses of content that may be barred by implementation of the broadcast flag even though they are otherwise reasonable and legal. Our inquiry has focused on whether there is a way to think about technology and law that recognizes existing patterns of reasonable consumer uses and allows for new, as-yet-undiscovered reasonable uses to emerge. It seems to some people that the law should apply the first sale and fair use doctrines to digital content regardless of the digital rights management scheme imposed by the rights holder. At the same time, many have stated that the law should not permit anyone to make and distribute unauthorized copies of digital content to the public just because technology makes this possible. There are no answers to this set of concerns in the FCC's ruling.[49]

---

[47] FCC Report and Order, p. 10 n47.

[48] Some argue that this expense and confusion will actually slow down the DTV transition.

[49] Other very difficult questions not addressed by the current rule include: What will the consequences of license and other obligations imposed on home network devices be for consumers? Who, if anyone, will have the affirmative obligation to review these agreements on behalf of consumers? Who, if anyone, will have the affirmative obligation to review the impacts of "approved technologies" on personal privacy? Many consumers are concerned about the effect on their privacy of the proposed flag scheme. Having the ability to offer consumers finely-tuned rights packages carries with it the potential ability to know what each individual is watching, where that person lives, and how long they watch what they watch—information that broadcasters do not now collect.

CDT recognizes that it is very difficult to state what are "reasonable consumer uses" and what are not. Nevertheless, flag implementation should adequately recognize legitimate consumer demands and leave room for future innovation.

3.5. Public Interest Values

Implementation of the flag could have a negative effect on important public values such as fair use, access to public interest/educational content, and access to public domain materials.

The "fair use" questions are difficult, and are closely related to the reasonable use concerns we raised in the last section. "Fair use" is a specific legal category, protected under the First Amendment. Determining whether a particular use of copyrighted content is fair use is a case-by-case, fact-specific, and often-subjective inquiry. For this reason, it is extremely difficult to "code" the legal principle of fair use comprehensively into any copy protection scheme. Moreover, an attempt to "encode" fair use as it is today might inadvertently block future uses that would be deemed "fair." Indeed, encoding fair use might itself stifle innovation. However, it is not sufficient to say "it is too hard" to "code" fair use, and therefore block all reasonable consumer uses—including fair uses. To do so would allow technical code to amend legal code (i.e. the rules, however ill-defined, of fair use). We believe a credible point has been raised that mandating technologies that effectively prohibit what would otherwise be fair use of DTV content raises copyright policy and First Amendment concerns.

Additionally, some believe the flag ruling raises other important free speech values concerning access to educational and news content (and content already in the public domain). While some proponents of the broadcast flag say that they do not intend that such content will be flagged, the FCC rule clearly contemplates flagging of news and other public interest content. The decision of the Commission on this point raises serious concerns. The rationale for flagging news and other ephemeral content, which has limited value after its initial distribution, is particularly unclear, and concerns about fair use are acutely felt for news and public affairs.

Public-interest advocates raise other concerns. Compared with the regular version of any device, the "compliant" version will have many new ways of failing. Equipment companies will have to staff help-desks and fund higher support costs. Also, compared to the regular version, the compliant version may have more versions, more customization features, and more internationalization issues, and will therefore be more expensive to keep in inventory. Finally, some approved technologies might collect information about users and their viewing habits—perhaps in part to promote security—raising privacy concerns (and creating potential data privacy liability for manufacturers under the EU Privacy Directive or other similar laws).[50]

3.6. The Thorny Question of FCC Jurisdiction

[50] For example, technologies that allow people to securely distribute a program within a registered home network, might do so by requiring registration of all the televisions, computers, etc. within that home network. Then they might check the use of content on that network. That in turn might enable a content provider to gather and match information about a person's viewing habits.

The Notice of Proposed Rulemaking issued by the FCC in connection with the broadcast flag proceeding sought comment on "the jurisdictional basis for Commission rules dealing with broadcast copy protection."[51] It is fair to say that the FCC's jurisdiction in this area is far from certain.[52] Indeed, the FCC devoted more than five pages of its ruling to explaining why it had jurisdiction to issue such a set of rules, and appears to be anticipating near-term challenges to its assertion of rulemaking authority. The issue of jurisdiction is critical. Without appropriate authority the FCC decision is vulnerable to being challenged in the courts—and if struck down, it will be up to Congress to revisit the flag decision and grant the FCC authority.

This section briefly describes the jurisdictional issues that have been raised in the broadcast flag proceeding. Three main categories of concerns have been raised.

Does the FCC have clear statutory authority to act?

A starting point for analysis is the Communications Act of 1933 (amended in 1996), whose general purpose was to "make available...to all the people of the United States, a rapid, efficient, nationwide, and worldwide wire and communication service with adequate facilities at reasonable charges."[53] Pursuant to the Act, the Commission has exclusive jurisdiction to regulate all US radio transmissions, and exercises regulatory authority over all broadcasting mediums—including television.

Title III of the Act covers DTV issues, including broadcaster eligibility for DTV licenses, DTV signal quality, and DTV ancillary and supplementary services. Critics of the FCC's assertion of authority in the flag proceeding have said that this DTV-related Title cannot be extended to cover manufacturers because it is explicitly limited to broadcaster issues, and have argued that in the absence of explicit statutory authority the Commission may not act.[54] The MPAA has responded that Title III confers *direct* authority on the Commission to prescribe

[51] FCC Notice of Proposed Rulemaking, p. 3.

[52] As Philips has pointed out, "key Members of Congress are split about the FCC's jurisdiction in this area. Some members of Congress [Hollings and Tauzin] believe that the FCC has authority to impose broadcast flag regulations while others believe that such regulation is outside the FCC's purview [Leahy and Sensenbrenner]." Comments of Philips Electronics North America Corporation, to the Federal Communications Commission, in the matter of Digital Broadcast Copy Protection, (December 2002), p. 32. (Hereinafter cited as Philips Initial Comments.)

[53] Robert Sears McMahon, *Federal Regulation of the Radio and Television Broadcast Industry in the United States 1927-1958* (New York: Ayer Company, 1979), p. 93.

[54] See Philips Initial Comments, p. 32: "In prior instances in which the FCC has regulated consumer electronics devices, Congress has enacted enabling legislation that grants the FCC specific authority over narrowly defined features and functions of those devices. Only thereafter does the FCC promulgate regulations." A recent DC Circuit opinion in the context of the FCC's August 2002 mandate that, on a phased-in basis starting in July 2004, all televisions sold in the United States contain a digital tuner, relied heavily on a specific source of statutory authority for FCC's regulatory action. The DC Circuit rejected the Consumer Electronics Association's claims that the FCC lacked jurisdiction, concluding that the Digital Tuner Order was a reasonable exercise of the FCC's authority under the All Channel Receiver Act. *CEA v. FCC*, No. 02-1312 (D.C. Cir., October 28, 2003). The Court also noted that the "[DTV] transition is not a market-driven migration to a new technology, but rather the unambiguous command of an Act of Congress." Slip. op. at 15.

rules requiring DTV reception equipment to have the ability to act in response to flagged content.[55]

The FCC, for its part, did not assert in its ruling that it had direct, explicit statutory authority to regulate equipment manufacturers. It did, however, reject the argument that an explicit grant of authority from Congress is required for it to act—although it "recognize[d] 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...jurisdiction over consumer equipment manufacturers in this manner."[56]

Critics of the FCC's rule also argue that it is, in effect, a rule about enforcing copyright protection. The FCC has stated that it has no authority over copyright law, and there is ample Congressional copyright legislation already in existence that does no devolve any administrative power to the FCC.[57]

In the absence of an express statute providing it with authority, can the FCC assert ancillary jurisdiction?

Under current caselaw, where no statutory authority exists providing the FCC with jurisdiction, the FCC may nonetheless act to "further the achievement of long-established regulatory goals."[58] The battleground for future jurisdictional discussions about the broadcast flag regulations will likely be the appropriateness of the FCC's exercise of such "ancillary" jurisdiction.

The MPAA has asserted that the FCC clearly has ancillary jurisdiction in this area, and that the exercise of such jurisdiction is necessary in order for broadcast to be able to compete on a level playing field with satellite and cable.[59] In responding to its critics, the FCC has taken a strong stance in support of its ancillary jurisdiction over equipment manufacturers. First, the FCC asserts that ancillary jurisdiction need not be "necessary" to the FCC's statutory responsibilities but can exist, instead, where it is "*reasonably ancillary* to the effective performance of [its] various responsibilities"—a different legal standard.[60] The Commission finds support in its general jurisdictional grant over broadcasting, which it believes covers the subject of this regulation,[61] and asserts that television receivers are within the scope of

---

[55] MPAA Joint Comments, p. 31-34 (no emphasis in original).

[56] FCC Report and Order, p. 17.

[57] Perhaps in recognition of this potential jurisdictional argument, the FCC changed the name of its rulemaking from "copy protection" to "content protection" when it issued its final rule.

[58] *FCC v. Midwest Video*, 440 U.S. 689, 698-700 (1979) (Hereinafter cited as "Midwest Video II").

[59] MPAA Joint Comments, p. 31-39.

[60] The FCC cites *United States v. Southwestern Cable Co.*, 392 U.S. 157 (1968) ("Southwestern Cable") in support of this standard. FCC Report and Order, p. 14 n.70 (emphasis supplied). The FCC restates the test for ancillary jurisdiction as one that looks for a "nexus"—a connection—between the FCC's statutory obligations and the expanded jurisdiction, rather than a floor of "necessity" for ancillary authority to exist (the test urged by FCC's critics).

[61] Specifically, Section 1 of the Communications Act states that the FCC is created "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so

the FCC's authority. Second, the FCC argues that its responsibility for the overall DTV transition dictates that it must act now. The Commission presents a laundry list of factors that it believes justify its exercise of ancillary jurisdiction in this area.

Critics of the FCC's exercise of ancillary jurisdiction have argued that such an assertion of power may only be made when "*necessary* to ensure the achievement of the Commission's statutory responsibilities."[62] It seems quite possible that courts reviewing the flag regulation would find that the flag regulation is not in fact necessary in order to put into effect the statutory requirements placed on the FCC for effecting the DTV transition.

Should the FCC have refrained from acting to allow for a national debate to take place in the legislature?

Those questioning the FCC's jurisdiction have argued that in the face of jurisdictional uncertainty, and in the absence of consensus on the necessity, effectiveness, and impacts of the flag scheme, it would be prudent to wait for a direct grant of statutory authority from Congress.

In response, the FCC asserts that even though "this may be the first time the Commission exercises its ancillary jurisdiction" in this way, "the nation now stands at a juncture where such exercise of [ancillary] authority is necessary."[63] The FCC suggests that to await a Congressional grant of authority would simply allow additional "legacy" (uncontrolled) DTVs to reach the marketplace, and states that the broadcast flag regime is essential in order for high-quality digital programming to be provided via free over-the-air broadcast.[64]

It is likely that these and other jurisdictional arguments will be raised in court proceedings widely expected as of this publication in early December 2003.

---

far as possible, to all the people of the United States…a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges." 47 U.S.C. 151. Section 2 of the Act gives the Commission authority over all interstate communication by wire or radio. 47 U.S.C. 152(a). The FCC also points to a general liberty of action presupposed in the Communications Act: "The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions," 47 U.S.C. 151(I), and relies on the fact that the definition of "wire/radio communications" includes "all incidental 'instrumentalities, facilities, apparatus and services' that are used for the 'receipt, forwarding, and delivery' of such transmissions." FCC Report and Order, p. 29. The FCC's argument begs the question: in enacting the Communications Act, did Congress intend the FCC to have authority to regulate consumer electronics and information technology devices? The fact that the Act contains broad definitions of "instrumentalities, facilities, apparatus, and services" does not answer that question, nor does it mean that Congress intended to give the FCC limitless authority to regulate anything that might fall within a possible interpretation of the Telecommunications Act.

[62] Midwest Video II, 440 U.S. at 706.

[63] FCC Report and Order, p. 17-18.

[64] FCC Report and Order, p. 16-17.

4. ISSUES FOR POLICY-MAKERS

4.1. Addressing Concerns with the Flag

Based on what we have learned in our dialogue with key stakeholders, CDT believes that the broadcast flag rule adopted by the FCC mitigates some of the important concerns addressed above, while leaving others un-resolved. We believe that the appropriate resolution of some of the issues deferred to the follow-on rule-making, combined with attention to important values in the way the rule is carried out could improve the rule consistent with its stated goals. Here are our suggestions, keyed to the discussion sections above:

Innovation concerns

- *Specific, objective functional criteria should be adopted and used instead of the arbitrary interim process.* Such functional criteria should be rooted in clear goals for the flag, should be reasonably easy to understand, and should permit developers to self-certify. They should be an exhaustive list of specific objectives rather than the broad, incomplete list of general factors provided in the interim process. For example, criteria could include "effectively frustrates the Internet distribution of protected content to the public" or "effectively frustrates the Internet distribution of protected content to more than *x* devices" (where *x* is a somewhat arbitrary but reasonable number).

- *The final Authorization process should permit self-certification* to allow for relatively fast and simple addition of compliant technologies to the list of Authorized Technologies.

- *Quick, independent arbitration should be established* for cases where a self-certification is challenged. Unlike in the interim process, the FCC should not act as the arbitrator. A representative arbitration/review board, with participation from the content, IT, CE, and consumer points of view, might be a better solution.

- *It should be made clear in the criteria for technologies themselves that software solutions are on the same footing as hardware solutions* in terms of eligibility for being approved technologies. Software solutions offer several advantages; for example, software would be upgradeable if breached and could be implemented inside portions of a personal computer (rather than affecting the whole).

- *Any list of Authorized Technologies approved under the interim process should include multiple technologies, and should not permit licensing terms that prohibit interoperability.* The terms of any private license agreements for Authorized Technologies (and the associated encoding rules for these technologies) should be made public in an easily accessible way.

Such steps will promote competition and creativity and will ultimately provide consumers with a greater array of choices.

Reasonable consumer use concerns

Consumer and computer user concerns about reasonable uses are closely linked to issues of innovation addressed above. Additional suggestions include:

- *Secure online transmissions*, to limited numbers of addressees, should be clearly permitted.

- *Consumer input should be incorporated in the authorization process*, including regarding the details of the encoding rules associated with Approved Technologies. In some cases, specific rules would be most appropriate, subject to public comment. One goal of such input would be to ensure that a breadth of technologies supporting a variety of evolving consumer uses are available under the flag regulation.

- The FCC should establish a process for *periodic oversight of license limitations* associated with Approved Technologies, which may impact consumer use.

- To support such a process and to more broadly promote public awareness, the authorization process should *require transparency for Authorized Technology licensing agreements.* The agreements (and the associated encoding rules for these technologies) should be made public in an easily accessible way (subject to protections of proprietary terms).

- *Any definition of "personal digital network environment"* should allow for expansive and flexible consumer uses of content and not restrict future business models..

Public interest concerns

- *The failure to exempt news and public affairs material from the full range of flag regulation protection should be reconsidered.* The encoding rules for Authorized Technologies should be sensitive to the role of such publicly important content in public discourse.

- *A standing oversight body*, made up of consumer representatives as well as industry representatives, should be constituted to provide advice with respect to public interest issues, including but not limited to fair use questions.

The follow-on proceeding launched by the FCC provides the opportunity to address several of these issues but should be expanded to deal with the remaining areas, including standing oversight and fair use and the protection of public interest content—particularly ephemeral content such as news broadcasts. These issues have not received a full hearing before the Commission or other policymakers to date.

4.2. Other Concerns

Even with the improvements made by the FCC in its first flag rule, and even if the additional changes we propose are made, other concerns raised by the flag will remain unresolved:

Precedent set by the flag for regulation of the computer - Personal and business computers are capable of demodulating TV signals and serving as "downstream devices"

and therefore will be impacted by the flag rule. Computers are (or will be) a key component of many consumer home networks. They are also a source of enormous innovation and economic growth in this country. Their essential feature has been the open platform, which permits innovation. We are concerned about the precedent the flag proposal will set for regulating the computer.

Precedent set by the flag for technology mandates - While many argue the flag approach approved by the FCC is narrowly focused, it is unquestionably a technological mandate: under the regulations, all machines handling DTV content will have to adhere to a particular set of rules. Public policy to date has largely resisted such mandates, especially with respect to computers, for reasons that remain compelling.[65] In an era of rapid change and technical complexity, government technology mandates have been heavily resisted in part due to the slow speed and inflexibility of regulation, as well as the expertise that resides in the private sector rather than the government. We share this concern about technology mandates, and recommend that policy makers continue to follow the no-tech-mandate principle.[66]

No consumer choice due to market dominance by one or a small number of protection technologies - Although we have argued in favor of authorization of multiple protection technologies and self-certification of copy technologies, we are aware that the investment required and the already-entrenched position of 5C may mean that new protection technologies do not emerge for some time—if at all. This will be bad for consumers. Consumers will benefit from having choices of protection technologies and from competition among technologies. While we have suggested more specific functional criteria and a minimum for the number of Authorized Technologies as measures to promote competition, there is a chance this will not be sufficient.[67]

Few new consumer uses permitted, with possible retrenchment over time - Similarly, we are worried that under the flag scheme, manufacturers will lose the incentive (or legal ability) to develop new uses of content that will comply with the broadcast flag regulations. Again, this is not good for consumers, for innovation in this country, or for the long-term health of the content providers, who benefit from new and innovative markets for content delivery and use.

Content protection and piracy problems remain - As has been noted, the broadcast flag will be limited in its effect. It is technically quite easy to circumvent. The easy digitization of

---

[65] As the head of the RIAA said in announcing an agreement with key IT trade groups in early 2003, "Another important plank in this agreement is a firm commitment to opposing government-imposed technological mandates. The RIAA believes in innovation. And we believe that consumers in the marketplace, not the government, should decide which technological innovations will thrive." Hillary Rosen, Business 2.0, http://www.business2.com/articles/mag/0,1640,48572,00.html.

[66] This model has been codified in part in the DMCA, which states that manufacturers of computers and consumer electronics products have no obligation to ensure that their devices respond to particular copy protection technical measures (Section 1201(c)). Many view this as a critical element of the balance struck under the DMCA. The Act does feature an analog mandate for manufacturers of VCRs to use Macrovision (which prevents VCR-to-VCR copying) in their devices (Section 1201(k)).

[67] At the same time, given the slow sale of DTV receivers and the fact that most Internet users cannot yet easily transfer large HDTV files, there is some time to promote consumer choice and avoid lock-in of a single technology.

analog signals—which must remain available as they are essential to ensure that hundreds of millions of existing televisions, VCRs, and DVD players continue to operate—will be the source of digital copying for years to come. A huge number of video programs already exist in unprotected digital form and can be traded online. Regardless of its effect as a hurdle against easy copying of DTV broadcasts by unsophisticated users, the flag regulations will do little to address these other very serious potential sources of copyright infringement. Rather, it must be viewed as only one part of a much broader debate about protecting content in the digital age.

Thus, even with the further changes to the flag that we suggest, significant concerns about consumer uses, innovation, effective copyright protection, and government regulation of computing and consumer electronics more generally would remain unresolved.

4.3. Non-Flag Protections for DTV Content

We have explored with our dialogue participants options for addressing concerns about video piracy that do not involve an implementation of the broadcast flag. Notwithstanding the FCC's action, and given the limits of the flag regulations in stopping unauthorized redistribution, we believe that a "three-legged stool" of approaches taken together hold out great promise for having a broad impact on digital piracy online: Enforcement, Education, and new Economic Models.

Enforcement - Current copyright law provides copyright holders with very significant enforcement tools. Laws in the U.S. against copyright infringement carry substantial criminal and civil penalties—but are rarely enforced today against many online infringers. CDT believes that it is unhealthy for our country, and unfair to copyright holders, for millions of computer users to routinely violate the law of the land. The recent efforts by the recording industry to sue suspected infringers who use peer-to-peer file-sharing systems has already had a major effect on public awareness, and we believe could mark a turning point in music file-sharing if it is accompanied by serious educational efforts and legal downloading alternatives.

To be effective, legal action must be coupled with the introduction of attractive legal alternatives for online content distribution as well as broad education efforts, and must be pursued consistent with due process and proportional penalties. Such legal action by the video industry, while undoubtedly unpopular, could go a long way towards raising awareness about copyright issues among consumers and computer users. CDT believes that targeted enforcement—consistent with due process, and coupled with education and attractive legal alternatives to digital piracy—could have a substantial deterrent effect on piracy.[68]

Education - Many content companies are frustrated because they believe that consumers—and young people in particular—do not seem to care about copyright. Enforcement efforts will help address consumer apathy, but large-scale public education is needed to transform the awareness created by enforcement into a genuine understanding by consumers of their rights and responsibilities under copyright law. The Business Software Alliance, for example, has made a good deal of progress through a concerted public

[68] *See, e.g.,* CDT Testimony before the Senate Commerce Committee (September 2003).

campaign of awareness and learning about software copyrights; the video content industry should embrace a similar approach.

Several educational efforts are already underway. The recent public awareness campaign and commercial announcements by the motion picture industry are a fair start. The collective rights organizations, the American Society of Composers, Authors, and Publishers (ASCAP) and BMI, have spent a great deal of money educating students and practitioners for many years about copyright law. Universities are increasing their copyright education efforts. The Copyright Association of America hosts town meetings and conferences about copyright, and many other trade associations do the same. These efforts should continue, but we believe education will be most effective over time if people are able to hear from traditional sources of objective consumer information as well as the affected industries.

New Economic Models for Digital Distribution - The conventional wisdom among copyright holders has been: "You can't compete with free." As the music industry is finding, new digital distribution systems provide ways to compete with free. Consumers have shown that they believe that easily searchable, downloadable, value-laden content is worth paying for online. Faced with the choice of purchasing a legitimate copy of a valuable piece of entertainment using a high-quality service and at a reasonable price, or illicitly downloading the same content over an error-prone, unfriendly connection with the risk of an enforcement action, we believe that the majority of consumers will gravitate towards the higher-quality, lawful offerings of the major content producers. The incredible success of Apple's iTunes Music Store, which quickly surpassed 10 million downloads of major-label songs and albums despite serving only a small percentage of consumers, and which has now successfully expanded into the broader Windows market and prompted an array of competing services, is a powerful demonstration of this point.

While the music industry was caught off guard by the spread of online file sharing—and as a result took several years to develop legal alternatives with satisfactory copy protection schemes even as a file sharing "culture" developed online—the video content industry has the opportunity to preempt online sharing of copyrighted video content by offering attractive legal alternatives from the start. The studios have begun moving in the direction of offering high-quality, value-added downloads. For now, these services are hampered by the same bandwidth constraints that are keeping video piracy in check, but as access to bandwidth in the "last-mile" grows, studios must be prepared to strengthen and expand these services.

4.4 Broadcast Encryption at the Source

Although the FCC roundly rejected alternatives to the broadcast flag, other technical approaches to the copy protection problem faced by the video industry still merit consideration. Foremost among them is broadcast encryption—permitting the encryption of DTV signals at the source rather than broadcasting them "in the clear." It is widely agreed that encrypting the DTV signal would provide more effective protection than the flag scheme. Permitting marketplace use of broadcast encryption might also avoid the troubling technology mandate implicit in the flag and its authorization process for protection technologies. At the same time, broadcast encryption leaves unresolved questions about just what systems will be permitted to decrypt DTV, what licensing restrictions will apply, and consequently what consumer uses will be permitted. While CDT believes these are serious unresolved issues, the costs and benefits of this approach should be explored, and not rejected out of hand because of a possibly outmoded vision of broadcast—especially since

the vast majority of American households subscribe to cable or satellite TV, where video content is delivered in protected form.

Another technical approach that might be useful—if only as a stopgap measure—would be to require that all DTV broadcasts be transmitted in high-resolution formats, rather than as narrow slices of a channel's spectrum. Huge files are very difficult to trade online, and if the movie industry wants to slow piracy it could do that through keeping file sizes large.

5. SUMMARY AND CONCLUSION

The broadcast flag approach approved by the FCC is a complex and important move designed to protect DTV broadcasts from unauthorized redistribution, with serious potential implications for consumer uses, technological innovation, and content protection writ large. The FCC's approval of the flag is both an important milestone and the opening of the next phase of the digital copyright debate. The previous sections have provided a careful description and analysis of the flag approach and the arguments for and against it. This section summarizes our major findings.

F.1 Protecting copyright in the digital age is important for both consumers and content owners; failing to protect broadcast content can have major implications for the availability of high-quality digital broadcast programs; and genuine fears have been raised about unauthorized redistribution of unprotected digital TV.

The country's transition to broadcast digital television, slated to occur by 2006, is part of a broad content protection challenge facing movie studios and other video producers. DTV programs, broadcast with no protections, are one source of unprotected digital content that will make it increasingly easy for people—especially those with broadband connections—to share digital TV programs and movies. The creators and owners of video content understandably fear future widespread piracy of video online, and want to avoid its risks. The "broadcast flag"—a combination of technical standards and federal regulations designed to mark and protect digital television—is a response to the DTV piracy threat.

The broadcast flag approach is, we believe, a genuine first attempt to resolve these issues in the context of a national tradition of "free" over-the-air television broadcast. CDT, based on its dialogue with key stakeholders and its reading of the FCC's Report and Order, understands the goals of the flag to be to:

- prevent the "indiscriminate redistribution" of protected broadcast content over the Internet;
- allow many different market offerings and new content delivery mechanisms, consistent with content protections; and
- allow many reasonable uses of content, including the ability to copy freely within the home or onto physical media, so long as done in a way that does not allow indiscriminate redistribution online.

We perceive broad agreement among the flag's supporters – as well as the FCC – that the primary goal of flag regulations is to prevent widespread online redistribution of digital content. There also appears to be agreement that many reasonable uses of content—including unlimited consumer redistribution within the home network and copying onto physical media—should be permitted under the flag. From a consumer perspective, these are both welcome.

F.2 The broadcast flag approach creates many legitimate concerns for television viewers, Internet users, and industry groups. The flag approach has the potential to restrict reasonable uses of content by viewers, hinder innovation, and impose costs that outweigh the benefits of the limited copy protection provided by this approach.

The main concern about the flag rule is that it fails to meet its stated goals because it provides little firm guidance about what consumer uses and future technologies will be permitted. Most critically, the interim process for approving technologies permitted to handle flagged programs is highly subjective. As a result, television viewers can reasonably fear that implementation of the flag –

- might prohibit reasonable future uses of programs or movies, particularly digital uses like distributing a program in a home entertainment system, emailing a program, or taking a small excerpt of a program;
- will impose new costs on them as they will be required to use flag-compliant televisions, DVD players, computers, or digital recorders to record and view flagged programs;
- could hinder broader use of news or public affairs programs; and
- could hinder innovation in new systems for delivering and using video content, which will now be subject to a gatekeeper approval process.

A major element of these concerns is that implementations of the flag rule may "leave out the Internet." While unlimited physical copying of programs is apparently to be allowed, it remains unclear whether emailing programs or taking digital excerpts or any number of reasonable online uses will be possible in practice—even if they can be done in ways that prohibit widespread copying.

To its credit, the FCC report in principle supports secure Internet applications. Proponents of the flag are among the first to argue that studios and other content producers will want new delivery mechanisms. Unfortunately, the procedures in the broadcast flag regulations do not give the public guarantees that in fact these future new applications will be permitted—a concern which the execution of the interim approval process and the follow-on proceeding together have the potential to help address.

F3. The ruling recently handed down by the FCC includes some important, consumer friendly modifications to earlier proposals, but the Commission put off until its follow-on proceeding consideration of many of the most important issues.

Significant, consumer friendly revisions to the initial MPAA proposal incorporated by the FCC include:

- clarifying the purpose of the rule as limited to preventing indiscriminate redistribution of protected content online and as providing a speed-bump rather than as a fool-proof method of protection;
- explicitly stating the Commission's willingness to consider software-based protection measures on equal footing with hardware measures;
- specifying an "ordinary user" standard for robustness; and
- including consumer-oriented factors among the considerations in assessing new technologies for authorization.

At the same time, many of the most difficult questions regarding the flag approach center around the eventual process for authorizing new protection technologies. The Commission's interim process does not provide an adequate substitute or response to these concerns, and the difficult issues surrounding authorization remain up in the air. In some respects, this state of affairs represents the worst of both worlds for consumers, who are

faced with a flag regulation now and only a promise for future procedures to check its most troubling features.

Other important issues which have been deferred by the commission include the scope of a proposed "personal digital network environment" within which free redistribution of protected content would be allowed, and questions regarding the impact of the rule on open source media applications.

F4. Appropriate resolution of issues that the FCC has deferred to its further rulemaking could help address many of the outstanding concerns with the broadcast flag, particularly if the FCC creates more focused objective, functional standards for what devices and uses will be permitted by the flag regulations, and if the FCC ensures that the final process for certifying permitted technologies is open and publicly-accountable.

There is a path to addressing many of these concerns. The goal of diverse delivery mechanisms could be better reached, and fears about the flag could be mitigated, by creating clear objective criteria for permitted future uses. In future versions of the flag regulations emerging from the FCC's follow-on proceeding and perhaps other venues, we recommend specific steps, including:

- Specific, objective, functional criteria should be used instead of the general and incomplete guidelines provided in the current interim approval process. Such functional criteria should provide clear guidance about the kinds of uses and technologies that will be authorized. They should be focused on the goal of preventing indiscriminate digital redistribution. They should reflect the other goals of the flag including allowing diverse consumer uses of content and facilitating innovation, they should be reasonably easy to understand, and they should permit developers to self-certify.

- Further steps should be taken to mitigate concerns about reasonable uses, the future contours of "fair use," and access to news and public affairs programming. At minimum, some procedure for addressing these issues and some form of standing oversight should be part of any flag approach to assess the effect of flag regulations on existing reasonable consumer uses, on uses and devices yet to be invented, on home networks, and on public values. We believe answers to these questions will be essential for the long-term viability of any flag system.

Despite the FCC's stated reservations, we believe exploration should continue of "encryption at the source" as a potential way to address many of the concerns with the flag. Broadcast encryption provides more secure protection and could reduce concerns about technology mandates (as the government need not mandate the encryption used). However, it leaves open many of the same questions about permitted uses downstream raised above. Still, we believe the approach might yet provide a "win-win" compromise that has not received a full discussion among those debating the flag or before the FCC.

F5. Even if these issues are addressed, the flag approach will still pose unresolved concerns regarding technical regulation of computers and the Internet by the government, the impact of regulations on innovation and future consumer uses, and the definition of "fair use" and other copyright doctrines in the digital age. The flag system also leaves unresolved other serious copy protection problems for television content.

We note that even the steps we propose will not address all of the outstanding concerns with the flag. These include:

- The precedent set by the flag for technology mandates - The flag sets a precedent for regulation over computing technology that is understandably troubling to those concerned about innovation and access to information supported by the open Internet and the general-purpose computer. While many argue the flag regulation is narrowly focused, it is hard to argue that it is not a technological mandate, particularly from the perspective of consumers who have had little to do with its creation. To date such government regulation—and particularly FCC regulation—of computer architecture has been highly disfavored for important public policy reasons.

- The limitation of consumer choice due to market dominance by one or a small number of copy protection technologies - The standardization of first-mover technologies on the list of Authorized Technologies may mean that new copy protection technologies will not emerge for some time—if at all. This will be bad for consumers and the content industry, which benefit from having many choices of content delivery and protection technologies.

- The restriction of new consumer uses, with possible retrenchment over time - There are minimal assurances in the current rules that Authorized Technologies will permit a range of reasonable uses in practice, and nothing prohibits technologies today contemplated as Authorized Technologies from limiting consumer uses in the future.

These are all serious issues that are not easily addressed within the current approach set in motion by the FCC's regulation and follow-on effort. We believe that—at a minimum—further discussion is needed to develop approaches to dealing with these concerns.

F6. Regardless of the future of the flag regulation in the follow-on FCC proceeding, and potential proceedings in the courts and Congress, the combination of enforcement of existing copyright laws, introduction of new economic models and digital delivery mechanisms, and continued consumer education holds out great promise to have a broad, long-term impact on online copyright infringement.

Finally, a "three-legged stool" of approaches holds great promise for a sustained impact on digital piracy online while avoiding many of the most controversial pitfalls of enforcing copy protections through imperfect technology protection mandates:

- Enforcement - US law provides copyright holders with powerful but rarely exercised enforcement tools against copyright infringement online. CDT believes that targeted enforcement—consistent with due process, and coupled with education and attractive legal alternatives to digital piracy—could have a substantial deterrent effect on piracy.

- New Economic Models for Digital Distribution - We believe that consumers will gravitate towards high-quality, lawful offerings that are affordable and provide them with adequate capabilities to use content. Studios have begun to experiment and are learning about what consumer want, and now have the opportunity to preempt online sharing of video content by offering attractive legal alternatives.

- Education - Large-scale public education is needed to transform the awareness created by enforcement and new legal alternatives into a genuine understanding by consumers of their rights and responsibilities. We believe education can be effective over time, especially if provided by traditional sources of objective consumer information.

More than any single technology regulation proposal we believe that attractive digital distribution, coupled with enforcement and education, has the greatest potential to curtail online infringement, reward creative production, and benefit consumers.

The broadcast flag approach is a serious response to real, though in some cases prospective, threats faced by the broadcast content industry in the digital age. It could also have broad effects on the ways in which consumers view and use information generally, and the ways in which companies develop new products and devices to communicate and use digital video content.

Objective, functional criteria and transparent, independent processes offer the best way to ensure that the flag is able to readily accommodate new technologies. Such an objective, process-based approach, carefully implemented and closely monitored, will prompt investment in new technologies without compromising the protection of valuable copyrighted works. New distribution models that involve the Internet will mean larger audiences, satisfied consumers, and dramatic innovation. For these reasons, and many others, it is in the interest of everyone involved in this debate to ensure that paths to change are clear and objective.

At the same time, even with clearer, more objective criteria the flag approach leaves big questions unanswered. Just as ten years ago we could not have foreseen how the Internet would develop, today, we cannot predict the paths of technological development. We need to ensure that the steps we take today to protect the legitimate interests of copyright holders do not stifle innovative models of digital distribution. We do not know what those future models might look like. We do know, however, that computing and the open Internet have fostered unimagined changes in the ways we communicate and share information.

CDT calls on stakeholders and policymakers to pursue an open-minded and forward-looking dialogue towards balanced responses to the immediate challenges raised by the broadcast flag. We also believe that far more must be done to resolve the broader unresolved issues about innovation, content protection, and the user-empowerment potential of the Internet. The polarization of the current debate has prevented adequate discussion. CDT looks forward to facilitating a more balanced conversation, along the lines suggested in this paper, that seeks to promote what we believe are important and widely-shared values.

##