

Table of Contents

SUMMARY.....ii

I. Introduction.....1

II. The FCC Has Already Correctly Articulated That Inhibiting Indiscriminate Redistribution Over the Internet Should Be the Goal of the Broadcast Flag Regime, and Further Attempts To Define a Personal Digital Network Environment Are Impractical, If Not Impossible, and Best Left to Copyright Law2

 A. Defining Scope by Reference to the FCC’s Articulated Goal for This Proceeding Meets the Needs That the Content Community Has Identified.....3

 B. Restricting Content Freely Distributed to All Consumers to a Difficult to Define PDNE Is Not Useful.....6

III. Methods for Certification of Content Protection and Recording Technologies Must Include Certification Based on Functional Criteria with Review by an Independent Body.....8

 A. The FCC Should Allow Full Self-Certification, Adopt Functional Criteria, and Act Itself as Arbiter of Certification Disputes9

 B. The Broadcast Flag and Cable Plug & Play Approval Systems Should Not Be Unified14

IV. Revocation of a Technology Should Be Considered Only When a Technology Has Been Compromised in a Significant and Widespread Manner and Be Based on Careful Balancing of the Harms to Consumers, Device Manufacturers, Broadcasters, and Content Providers16

V. Conclusion.....19

SUMMARY

The Business Software Alliance and the Computer Systems Policy Project (together the “IT Coalition”), by their attorneys, hereby submit their comments in response to the FCC’s Further Notice, which seeks comments on, among other things, the usefulness of employing a “personal digital network environment” concept to refine the scope of redistribution to be prevented, the procedures and criteria for certifying digital output and recording technologies, and the standards for revocation of the approval of such technologies.

The FCC’s goal for broadcast protection -- to inhibit the indiscriminate redistribution of DTV content over the Internet -- needs no further elaboration. This meaningful but flexible standard precisely tracks the content owners’ stated concerns without imposing rigid restrictions on consumer use of broadcast content. Attempting to refine the scope of protection by reference to an ill-defined “personal digital network environment” would stifle technological innovation rather than enabling appropriate Internet or other distribution of broadcast content.

Key to a successful DTV transition will be shaping and implementing the broadcast flag rules in a way that advances this proceeding’s goal of providing a meaningful “speed bump” to indiscriminate redistribution of broadcast content without suppressing the development of innovative technologies for use with DTVs. If the rules instead have the effect of chilling innovation, DTV products will be slower to market and higher in price, and consumers will be frustrated and less inclined to embrace the DTV transition. To ensure this does not occur, the FCC should allow technology developers, as at least one method of obtaining the approval of digital output and recording technologies, to self-certify (without the need for affirmative FCC approval) such technologies as compliant with an articulated set of functional criteria. Such functional criteria will provide technology developers with advance guidance and certainty,

thereby encouraging the development of a diverse array of technologies, while reassuring broadcasters and content providers that broadcast content will be protected to the maximum extent permitted by the rules. FCC review of self-certified technologies should be limited to proceedings triggered by a *bona fide*, non-frivolous objection to a technology, a limitation which will preserve FCC administrative resources for legitimate disputes. Finally, it is critical that the FCC retain, for the time being, final decision making authority to resolve objections to self-certified technologies. Only the FCC is currently well positioned to decide such controversies.

The systems for approving technologies for use with "Plug & Play" and broadcast flag devices should not be unified. Despite some conceptual similarities between the criteria for evaluating technologies under the two regimes, significant differences militate against unification. The Plug & Play regime is much broader in scope and involves much more detailed regulation than the broadcast flag regime. Moreover, the FCC's jurisdictional bases for regulating in each area are completely different. Finally, CableLabs -- the entity initially approving technology in Plug & Play -- is not the appropriate body to adjudicate disputes regarding over-the-air unencrypted DTV technology.

Finally, the IT Coalition urges the FCC to refrain in all circumstances from revoking digital output and protection technologies in a way that disables devices already in consumers' hands. Revocation of a technology (on a "going forward" basis) should only be considered when breach of the technology is widespread and significant, the technology vendor is unable to remedy the breach, and the breach has compromised the DTV platform to such a point as to destroy its commercial viability. If the FCC finds this to be the case, then it must weigh the harm to consumers and device manufacturers of revocation against the harm to content owners if approval of that technology is not revoked.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)
)
Digital Broadcast Content Protection) MB Docket No. 02-230

COMMENTS OF THE IT COALITION

I. Introduction

The Business Software Alliance (“BSA”) and the Computer Systems Policy Project (“CSPP”) (together, the “IT Coalition”) by their attorneys, hereby submit their comments in response to the *Further Notice of Proposed Rule Making* issued as part of the Commission’s first decision in the above-referenced proceeding.¹

Since 1988, BSA has been the voice of the world’s software, hardware, and Internet sectors before governments and with consumers in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates computer users on software copyrights and cyber security, advocates public policy that fosters innovation and expands trade opportunities, and fights software piracy.² CSPP is a public policy advocacy group comprised of the Chairmen and Chief Executive Officers from America's leading information technology

¹ Digital Broadcast Content Protection, *Report and Order and Further Notice of Proposed Rule Making*, MB Docket No. 02-230 (rel. Nov. 4, 2003) (“*Order/FNPRM*”).

² BSA’s members include Adobe, Apple, Autodesk, Bentley, Borland, CNC Software/Mastercam, Dell, Hewlett-Packard, IBM, Intel, Intuit, Macromedia, Microsoft, Network Associates, Sybase, Symantec, and Unigrahpic Solutions (an EDS company), as well as other companies.

companies.³ CSPP provides recommendations on public policies with a transformative impact on society, including digital rights management, export controls, international trade, privacy and networked world infrastructure and access.

As the IT Coalition noted in its initial comments in this docket, it is gravely concerned about piracy and committed to fighting it.⁴ BSA estimates that its members lose \$11 billion to software pirates annually.⁵ Indeed, BSA was established to fight piracy worldwide, and all the constituencies represented by the IT Coalition continue to deplore those that pirate copyrighted works. Individually and collectively, BSA's members and the companies represented by CSPP spend considerable resources pursuing pirates that illegally copy and distribute members' copyrighted products. In addition, BSA and CSPP support strong intellectual property laws both domestically and globally, and BSA helps governments identify and prosecute pirates.

II. The FCC Has Already Correctly Articulated That Inhibiting Indiscriminate Redistribution Over the Internet Should Be the Goal of the Broadcast Flag Regime, and Further Attempts To Define a Personal Digital Network Environment Are Impractical, If Not Impossible, and Best Left to Copyright Law

In the *Order/FNPRM*, the Commission requested “comment on the appropriate scope of redistribution that should be prevented.”⁶ As discussed below, the IT Coalition believes that the FCC has sufficiently articulated scope in the *Order/FNPRM* as “prevent[ing] indiscriminate

³ CSPP's members include Dell, Inc., EMC Corporation, Hewlett-Packard Company, IBM Corporation, Intel Corporation, Motorola Corporation, NCR Corporation, and Unisys Corporation.

⁴ Comments of the IT Coalition, in MB Docket No. 02-230 (filed Dec. 6, 2002) (“IT Comments”) at 2.

⁵ *Id.*, citing International Planning and Research Corp., *Seventh Annual BSA Global Software Piracy Study* (2002).

⁶ *Order/FNPRM* at ¶ 63.

redistribution” over the Internet.⁷ This goal meets the threat that the Motion Picture Association of America (“MPAA”) and others in the content community had identified in their comments,⁸ while ensuring that individual consumer behavior and enjoyment of DTV content are not inhibited.

As further discussed below, the IT Coalition opposes any effort to further refine the scope of protection by reference to some artificially defined “personal digital network environment” (the “PDNE”). Granular control of consumers’ enjoyment of over-the-air DTV could have substantially negative consequences for the DTV transition by causing consumers to delay or avoid entirely any use of new distribution forms that do not conform to their current viewing experience. On the other hand, setting the scope as inhibiting indiscriminate redistribution over the Internet will encourage the creation of new and exciting ways for consumers to enjoy DTV and thus promote the DTV transition while forestalling that future threat.

A. Defining Scope by Reference to the FCC’s Articulated Goal for This Proceeding Meets the Needs That the Content Community Has Identified

In discussing the concept of scope in the *Order/FNPRM*, the Commission noted that, “[i]n general, we believe that a flag based system should prevent indiscriminate redistribution of digital broadcast content.”⁹ The IT Coalition wholeheartedly endorses this goal statement and believes it sufficiently defines the scope of protection for the broadcast flag regime. The FCC is correct in taking this approach for a number of reasons.

⁷ *Id.* at ¶ 19. *See also* ¶¶ 4, 6, 10-12, and 34.

⁸ *Id.* at ¶ 14, *citing* Joint Comments of Motion Picture Association of America, *et al.*, in MB Docket No. 02-230 (filed Dec. 6, 2002) (“MPAA Comments”) at 12.

⁹ *Order/FNPRM* at ¶ 63.

First, as noted in the *Order/FNPRM*, the Commission's intent in adopting this goal was not to inhibit consumers from making copies for time shifting purposes or any commensurate consumer behavior.¹⁰ Rather, the Commission's clearly stated intent was not to interfere with any consumer actions that are permitted by the Copyright Act. The Commission left fully intact the applicability of copyright law principles, which would serve as the boundary for protection, in lieu of Commission rules:

Furthermore, the scope of our decision does not reach existing copyright law [T]he underlying rights and remedies available to copyright holders remain unchanged [T]his decision is not intended to alter the defenses and penalties applicable in cases of copyright infringement, circumvention, or other applicable laws.¹¹

Taking this approach allows the definition of scope to be sufficiently broad to permit future development of access to DTV in the many ways that are still unimaginable today. Such an approach also carves out the area in which redistribution is to be inhibited rather than doing the opposite by attempting to define narrow areas in which content may be copied and used.

Second, this approach also meets the concern over harms that MPAA articulated in its initial comments. There, MPAA stated as follows:

Because it is transmitted in the clear, digital broadcast television is subject to an extraordinary high risk of unauthorized redistribution over networks such as the Internet. The threat of such wide-scaled piracy, if not addressed, will lead content providers to cease making their high-value programming available over broadcast television.¹²

¹⁰ *Id.* at ¶¶ 9 and 10 (“This goal will not (1) interfere with or preclude consumers from copying broadcast programming and using or redistributing it within the home or similar personal environment as consistent with copyright law, or (2) foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution.”).

¹¹ *Id.* at ¶ 9.

¹² MPAA Comments at i.

Indeed, MPAA devoted extensive discussion in its Comments to outlining the threat of indiscriminate redistribution over the Internet.¹³ In the *Order/FNPRM*, the Commission acknowledged that while today “technological constraints will inhibit the redistribution of HDTV over the Internet,” it agreed with MPAA’s assessment that such unrestrained Internet redistribution, particularly on peer-to-peer file sharing networks, is the future threat that the FCC was attempting to address in this proceeding.¹⁴ The record is very clear that the problem the broadcast flag is intended to address is indiscriminate redistribution over the Internet.

Third, the approach to scope adopted by the Commission is consistent with the type of content that is being protected and the FCC’s intended level of effectiveness for the overall protection system. The broadcast flag system will be used to signal redistribution protection for free over-the-air DTV programming, which in this country is broadcast in the clear to approximately 108.4 million TV households in the course of an evening.¹⁵ As to the flag system’s effectiveness, the Commission noted that, assuming the flag was necessary, it was meant to serve merely as a “speed bump” against indiscriminate redistribution.¹⁶ Given these two factors -- the intentional widespread distribution in-the-clear of content and the level of protection intended for the system -- it makes little sense to make attempts, which will ultimately be futile, to draw artificial lines around consumers’ elusive “personal digital network environments.”

¹³ *Id.* at 6-10.

¹⁴ *Order/FNPRM* at ¶ 8.

¹⁵ See http://www.tvb.org/rcentral/mediatrendstrack/tvbasics/02_TVHouseholds.asp (last visited Feb. 13, 2004).

¹⁶ *Order/FNPRM* at ¶ 14.

A central goal of this proceeding, as well as a basis for the Commission's conclusion that it had jurisdiction to act, was to promote and foster the transition of the nation's broadcast television system from analog to digital. As noted above, absent regulation, the content providers and broadcasters had claimed that their fear of indiscriminate Internet redistribution would keep them from providing the high value content necessary to attract consumers to DTV. The Commission responded to this concern, citing its congressionally imposed responsibility to shepherd "the country's broadcasting system into the digital age."¹⁷ Over the years, based on marketplace developments, consumers have developed reasonable expectations for utilizing broadcast TV content. The FCC's definition of scope should leave this well functioning marketplace untouched except when necessary to meet the goal of preventing indiscriminate Internet redistribution.¹⁸

B. Restricting Content Freely Distributed to All Consumers to a Difficult to Define PDNE Is Not Useful

The *Order/FNPRM* seeks comment on the "usefulness of defining a personal digital network environment ('PDNE') within which consumers could freely redistribute digital broadcast television content."¹⁹ Such an exercise is in no way useful because regulations based on a PDNE approach would be disruptive of current consumer practices and expectations and would be inappropriate as a matter of substantive law.

¹⁷ *Id.* at ¶ 30.

¹⁸ *Id.* at ¶55 ("[W]e anticipate that technologies can protect content while facilitating consumer uses and practices. We also believe that technologies can promote consumer access to content, particularly in formats accessible to the blind and visually impaired.").

¹⁹ *Id.* at ¶ 63. As the Commission intimates, defining a PDNE would be a daunting task. In its previously filed comments, MPAA has focused on location in defining the PDNE as "the home or similar local environment." MPAA Comments at ii.

This proceeding has focused on protecting content from indiscriminate redistribution. By focusing on further, difficult to define constraints such as those based on location control, the PDNE is an attempt to protect current broadcaster business models rather than address the problem before the Commission. Given the increasing ubiquity of portable digital devices and secure communications across networks, no reason exists to limit consumers' use and enjoyment of DTV to a given location, or other artificially defined "environment," as long as indiscriminate redistribution is inhibited. In this country, consumer use and practices with respect to video, for example, have not been location based. A DVD will play just as well in a consumer's office, home, car as well as in a laptop on an aircraft. Similarly, a parent can transmit a digitized analog local news program to his or her child who is away at school. Location is irrelevant as long as the consumer is located within a wide, almost continent-sized, region.²⁰ Imposing artificial restrictions on consumer use based on a PDNE approach would, without a doubt, interfere with existing consumer expectations and uses.²¹ Further, a "one size fits all" definition of the consumer's digital environment, based on location or any other parameter, would not foster continued innovations in technology and corresponding evolution of legitimate consumer uses and practices. As long as DTV content is not indiscriminately redistributed, the Commission should not interpose itself and disrupt technological development and positive market forces.

²⁰ DVD pre-recorded movie discs are marked with a "regional code" so that they will only play on DVD players and DVD ROM drives that are set for that particular region. Regions generally correspond to continents. For example, Canada and the United States have been designated as Region 1. DVD movies marked with Region 1 will play on any machine set for that region. Region 2 includes much of Europe. A Region 2 DVD disc will not play on a device set for Canada and the United States but will play on one set for the European region.

²¹ The *Order/FNPRM* states that the goal of this proceeding is **not** to "foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution." *Order/FNPRM* at ¶ 10.

In addition, the attempt to define a PDNE is inappropriate as a matter of substantive law. The effort to regulate authors' rights in their works began nearly 300 years ago and has resulted in the copyright principles set forth in Title 17. Determining appropriate usage in an artificially defined PDNE would require the Commission to delve into copyright law, a role never assigned to it by Congress.

Defining scope as the inhibition of indiscriminate redistribution over the Internet removes any need to engage in a time-consuming and ultimately futile effort to define a PDNE. Furthermore, we support the FCC's statement that use of the Internet should not be foreclosed when sending digital broadcast content where robust security can adequately protect the content and redistribution is narrow.²² DTV adoption will only be advanced by not interfering with current consumer expectations and at the same time making available to consumers the quality and personal flexibility that digital technology provides. The resulting consumer demand will foster yet more innovation and efficiency. The interim scope approach strikes the right balance among consumers' reasonable expectations, the FCC's goal of establishing a "speed bump" to unauthorized redistribution of free over-the-air content, and avoidance of burdens on consumers and device manufacturers. It should be made final. The Commission should not create unnecessary complexity and concerns by attempting to layer PDNE-based restrictions on its already articulated scope goal.

III. Methods for Certification of Content Protection and Recording Technologies Must Include Certification Based on Functional Criteria with Review by an Independent Body

The IT Coalition's goal -- and one that makes good sense from a public interest perspective -- is to maximize the number of technologies meeting the scope definition

²² *Order/FNPRM* at ¶ 63.

established in this proceeding and ensure their availability to DTV product manufacturers. As discussed below, to accomplish this goal, it is paramount that at least one of the mechanisms for approving technologies be based on functional criteria with full self-certification and the opportunity for review by an independent body. If one of the methods adopted is based on open self-certification with a review process that utilizes functional criteria, the IT Coalition can also support adoption of the other criteria set forth in the BPDG Final Report at § 6.6.1 and Tab F-1. Adoption of such additional approval methods would allow for certification of technologies that may be adopted in the market based on considerations not fully comprehended in purely functional criteria, thereby furthering the goal of maximizing technology choices available to manufacturers. The IT Coalition's primary focus, however, is on functional criteria, since without such an approach, competition may be stymied and, with it, innovation denied a chance to flourish and consumers denied the benefit of more choices and lower prices.

A. The FCC Should Allow Full Self-Certification, Adopt Functional Criteria, and Act Itself as Arbiter of Certification Disputes

The Commission's interim process is an excellent first step in the creation of a system for approving Authorized Digital Output Protection Technologies and Approved Recording Methods. The interim process is an open one that calls for self-certification, although with Commission approval, and is based in large part upon objective, functional criteria. The FCC acts as the final arbiter in the interim process.²³ The IT Coalition believes that the FCC can readily transform this interim process into well-crafted and appropriate final procedures by making only minor changes.

²³ See Section 73.9008 of the FCC's new rules, *Order/FNPRM* at Appendix B (to be codified at 47 C.F.R. § 73.9008).

First, the final rules should continue to allow self-certification with an opportunity for non-frivolous objections but remove the requirement of FCC approval. In other words, unless a party files a legitimate objection with the Commission, an applicant's certification that its application meets the rule's requirements should be accepted as final without the need for a Commission determination. Eliminating the need for the Commission to rule on every application will speed the process and conserve FCC resources for those cases in which a genuine dispute arises over the efficacy of the technology. Full self-certification will also encourage the maximum number of manufacturers to offer compliant technologies, while preserving an appropriate opportunity to object, which will ensure that affected interests (content providers, device manufacturers, and consumers) are adequately protected against the entry of non-compliant technologies into the market.

Second, the permanent process should involve application of a more extensive delineation of the criteria to be applied. Providing appropriate criteria, including functional criteria for the certification of technologies, will promote the Commission's goal of fostering the DTV transition and will benefit consumers. The scope of this proceeding, no matter how stated, implicates technology. Once the Commission decided to adopt the broadcast flag system, it inevitably entwined itself in decisions about approval of existing and future technology for use in protecting DTV content against indiscriminate redistribution. The key to success, therefore, is to use the lightest hand possible in constraining design while, to the greatest extent possible, providing advance guidance to technologists and relying on market processes. The information technology community has long agreed that an important part of reaching that goal is to provide

functional criteria.²⁴ Accordingly, the IT Coalition urges the Commission to adopt the following criteria, which it believes are appropriate for the certification of output protection and recording method technologies:

1. Scope: The digital content protection method must provide reasonable constraints to impede the indiscriminate redistribution of Marked or Unscreened Content to the public.
2. Security: The digital content protection method must protect Marked or Unscreened Content, in conformance with the applicable compliance rules, when such content is transmitted to or recorded by one or more consumer devices, including but not limited to single and multi-function devices such as TVs, set-top boxes, game consoles and personal video recorders as well as general purpose devices such as PCs. A digital output protection method may be implemented in software or hardware or in any combination of the two.
3. Strength/Robustness: All cryptographic algorithms, cryptosystems, keys and secrets shall be of sufficient strength and bit length to render breach or compromise of content beyond the capability of an ordinary user using commonly available tools, while meeting applicable export control laws. The encryption algorithm should, in accordance

²⁴ As noted in the *Order/FNPRM*, Dell in this proceeding, and Microsoft and Hewlett-Packard in the cable set-top box proceeding (“Plug & Play Proceeding”), filed *ex parte* documents suggesting factors to be considered in adopting functional criteria for certifying protection technologies. See *Order/FNPRM*, ¶¶ 61-62 (citing *Ex Parte* Letter, filed by Dell, Inc., MB Docket 02-230 (Oct. 22[sic], 2003) (“Dell *Ex Parte*”); *Ex Parte* Letter, filed by Microsoft Corporation and Hewlett-Packard Corporation, CS Docket 97-80, PP Docket 00-67 (Aug. 8, 2003)). The proposals included herein have refined those proposals and constitute the IT Coalition’s consensus on the subject. Dell defined functional criteria as “a specification that defines a high-level framework outlining specific goals and objectives, without dictating or in any way preordaining the methods, processes and approaches that may be used to achieve those goals.” Dell *Ex Parte* at 1.

with common and well-regarded security practices, be published and subject to peer review. The algorithm must be such that detailed knowledge of a given implementation of the algorithm shall not, in and of itself, be sufficient to enable the production of circumvention devices. The method should require appropriate robust protection of compressed video Marked and Unscreened Content traversing a User Accessible Bus.

4. Rights/Interoperability: The digital content protection method must ensure that usage rights equal to or no more permissive than those delivered with the Marked/Unscreened Content (*i.e.*, control of indiscriminate redistribution to the public) are carried forward when the content is output to another device, including a device employing a different content protection system.

5. Authentication: The digital content protection method must be designed to ensure that Marked or Unscreened Content is output to or accessible by another device (including software) only if that device is compliant. This may be accomplished using *implicit* authentication, such as use of encryption keys that should be known only by compliant devices, or using *explicit* authentication, such as confirming the target device's credentials to protect the Marked or Unscreened Content consistent with the functional criteria prior to conveying a key for the Marked or Unscreened Content to the device.

The digital content protection method must securely manage the communication and distribution of any cryptographic keys or methods necessary for decrypting the Marked or Unscreened Content after output, using specific means to restrict such communication and distribution.

6. Compromise Recovery: It must be technologically possible to revoke and/or renew -- through either hardware or software or any combination -- the ability of an

individual device to receive Marked or Unscreened Content if the device's authentication keys or credentials have been compromised, including where a device is masquerading as a compliant device using the compromised device's keys or credentials. Revocation must be governed by appropriate rules, procedures, and safeguards.

Using functional criteria should make it unnecessary to exclude or include any particular protection technology based on its classification. If a certain technology meets the functional criteria, it is approved, whether it is called a DRM, link protection, or anything else. The public interest will be advanced by encouraging all manner of solutions that meet the criteria. This framework will provide the incentive for ongoing improvements and innovation. Content providers will be protected as long as the criteria are met; device manufacturers will have a larger universe of technologies from which to select based on price/performance; and, in the market, consumers will have a wider choice of DTV devices at lower cost.

Third, the permanent rules should designate the FCC as the final arbiter of certification disputes. The *Order/FNPRM* had suggested several possible arbiters: "the Commission, a qualified third party, or an independent entity representing various industry and consumer interests"²⁵ At the present time, the IT Coalition believes that the Commission is in the best position to resolve objections to self-certification. From the *Order/FNPRM* and the interim rules, it is clear that the Commission understands the issues related to over-the-air DTV content protection. No other existing and wholly unbiased entity has the capability to step into the Commission's shoes. While the IT Coalition's preference is eventual establishment of a number of technically qualified independent entities to arbitrate technology disputes that may arise, it will likely be some time before such entities emerge and become qualified. Despite the resource

²⁵ *Order/FNPRM* at ¶ 64.

burden such involvement may from time to time entail, the Commission is currently in the best position to arbitrate these disputes.

The IT Coalition urges the Commission to create the final certification rules by amending the interim rules to provide for full self-certification, inclusion of these functional criteria (along with means for approval based on other criteria), and establishment of itself as the final arbiter of certification disputes. Such actions will create an open, efficient process fostering competition, which in turn will benefit consumers with innovative and competitive DTV products. By making these changes to the interim procedures, the Commission will advance its goal of fostering the DTV transition.

B. The Broadcast Flag and Cable Plug & Play Approval Systems Should Not Be Unified

Last fall, in addition to approving the basic parameters of digital broadcast content protection, the FCC in the Plug & Play Proceeding adopted digital content protection standards for programming distributed by multichannel video program distributors (“MVPDs”).²⁶ Although the proceedings share some conceptual similarities, and while Commission decisions in one proceeding may have implications for the other, the two digital video protection technology approval processes should not be combined for at least four reasons.

First, a significant difference between the broadcast flag and Plug & Play content protection regimes is the type of material each involves. This proceeding covers only free over-the-air DTV. The MVPD systems at issue in the Plug & Play Proceeding, on the other hand,

²⁶ Commercial Availability of Navigation Devices, *Second Report and Order and Second Further Notice of Proposed Rulemaking*, CS Docket No. 97-80, PP Docket 00-67 (rel. Oct. 9, 2003) (“*Plug and Play Order*”).

supply several different types of content on a variety of terms and conditions.²⁷ Plug & Play affects not only retransmitted free over-the-air DTV, but also many other forms of video retransmitted by cable systems, including pay television, non-premium subscription television, free conditional access delivery transmissions, VOD, PPV, and Subscription-on-Demand transmissions.²⁸ The broadcast flag and Plug & Play regimes are similar only to the extent that neither imposes restrictions on copying free over-the-air DTV. The Plug & Play rules include separate copy control states for video products other than free over-the-air DTV.²⁹ This added complexity should not be imported into the broadcast flag technology approval process.

Second, the compliance certification process adopted in the Plug & Play Proceeding examines a series of technical factors unrelated to DTV content protection.³⁰ For example, in Plug & Play, there are a series of testing procedures designed to ensure compatibility of unidirectional cable products with the cable delivery system not relevant to broadcast flag.³¹ This difference alone militates against combined processes.

²⁷ *Id.* at § V.

²⁸ *Id.* at ¶ 65.

²⁹ Sections 76.1901-1908 of the FCC's new rules, *Plug & Play Order* at Appendix B (to be codified at 47 C.F.R. §§ 76.1901-1908).

³⁰ *Plug & Play Order* at ¶ 38.

³¹ *Id.* (“The test suite to be applied is intended to demonstrate that the subject device: (i) can tune and display scrambled digital services via the POD conditional access system; (ii) will not technically disrupt, impede, or impair delivery of services to cable subscribers; (iii) will not cause physical harm to the cable network or the POD module; (iv) will not facilitate theft of service or otherwise interfere with reasonable actions taken by cable operators to prevent theft of service; (v) will not jeopardize the security of any services offered over the cable system; (vi) will not interfere with or disable the ability of a cable operator to communicate with or disable a POD module or to disable services being transmitted through a POD module; or (vii) will not impede or impair control of content protection.”)

Third, the FCC's authority to regulate in this proceeding and in the Plug & Play Proceeding is derived from different statutory bases. The FCC's authority in the Plug & Play Proceeding is based on Section 629 of the Communications Act, which requires the Commission to assure the commercial availability of multichannel video programming converter boxes. In this proceeding, the Commission has relied on ancillary jurisdiction necessary to promote the DTV transition. Unifying two systems would be legally difficult when one relies on clear-cut legislative delegation, and the other involves derivative jurisdictional authority.

Finally, although the objective criteria and final arbiter of protection technologies were left undecided in the Plug & Play Proceeding, on an interim basis, approval of protection technologies was assigned to CableLabs, a private cable industry entity.³² That assignment would not work for the review of broadcast flag technologies and offers yet another reason to keep the two regimes separate.

IV. Revocation of a Technology Should Be Considered Only When a Technology Has Been Compromised in a Significant and Widespread Manner and Be Based on Careful Balancing of the Harms to Consumers, Device Manufacturers, Broadcasters, and Content Providers

In the *Order/FNPRM*, the Commission demonstrated appropriate sensitivity to the dangers of orphaning legacy equipment. While recognizing the superiority of encryption at the source, the Commission rejected that solution for DTV content in part because “we view[ed] the obsolescence of legacy equipment as particularly burdensome on consumers.”³³ There, the Commission was referring to the approximately 700,000 over-the-air DTV receivers that may be

³² *Id.* at ¶ 39. The Commission does exercise an appellate role in the process for approving protection technologies and anticipates that independent third party testing facilities will be available to certify compliance.

³³ *Order/FNPRM* at ¶ 24.

in consumers' hands.³⁴ As the FCC implements the new broadcast flag regime, it should accord equal sensitivity to DTV products purchased by consumers in the future, revoking approval of the digital output and recording technologies incorporated in those devices only (a) on a "going forward" basis (*i.e.*, de-authorization of a technology); (b) when a breach is significant and widespread; and (c) after a careful balancing of the harms of revoking or retaining the technology to consumers, device manufacturers, broadcasters and content providers. Setting the threshold at this level is important because revocation will be tantamount to the FCC intruding into the lives and homes of consumers to disable their newly acquired equipment at the same time the FCC is trying to promote these same consumers' adoption of and transition to DTV.

The Commission's selection of the flag system relied "on a balancing of the level of protection gained relative to the cost and burdens associated with the implementation."³⁵ No one involved in the BPDG process or this proceeding has urged that the standard that should be applied to devices is the absolute *prevention* of indiscriminate redistribution of protected DTV content over the Internet. Rather, inhibition of such indiscriminate redistribution is the goal. Even if the *Order/FNPRM* had required encryption at the source of DTV broadcasts and a higher level of robustness, the absolute prevention of indiscriminate Internet redistribution would still have been practically impossible to achieve.³⁶ Considering revocation only when a breach is

³⁴ "The cumulative DTV set-top box sales figure - sales from 1999 through June 2003 - has reached 397,512 units. That brings ATSC-receiving products, including both integrated sets and stand-alone set-top boxes, to 701,512 units." Press Release, CEA, "Digital Television Sales Flourish During First Half of 2003" (July 30, 2003), http://www.ce.org/press_room/press_release_detail.asp?id=10269 (last visited February 13, 2004).

³⁵ *Order/FNPRM* at ¶ 21.

³⁶ *Id.* at ¶ 19 ("We are equally mindful of the fact that it is difficult if not impossible to construct a content protection scheme that is impervious to attack or circumvention.").

both significant and widespread is consistent with the Commission's recognition that the flag system should provide a "speed bump" to indiscriminate redistribution.³⁷ Moreover, the ability of the technology vendor adequately to repair the breach should be an affirmative defense.

The best example of a widespread but not significant breach is cited in the *Order/FNPRM* as "instructive": the hack of the DVD content protection system. As the Commission noted, "[a]lthough the CSS copy protection system has been 'hacked' and circumvention software is available on the Internet, DVDs remain a viable distribution platform for content owners."³⁸ The same standard should apply here, *i.e.*, revocation should not be considered unless the breach is widespread and demonstrably significant. In determining whether the breach is demonstrably significant, the Commission should also require a showing that the breach has compromised the DTV distribution platform to such a point as to destroy its commercial viability.

Any revocation that does take place should apply only to subsequently-manufactured devices to minimize the risk of the Commission's inserting itself into consumers' homes and orphaning tens of millions of their compliant DTV devices, a very serious action. When the FCC adopted the broadcast flag regime, legacy DTV receivers only existed in one consumer device as opposed to the potentially numerous technologies that could be involved in any future revocations. To implement the broadcast flag system, output protection technologies will be needed not only in covered demodulator products, but in every digital device downstream from that product that receives marked content. If consumer adoption of over-the-air DTV continues at its current pace, before long millions of products will contain an authorized technology. If the adoption rate accelerates, tens of millions of consumers will be using devices that must connect

³⁷ *Id.*

³⁸ *Id.* at ¶ 20.

or play back via a specific authorized technology. If a technology were to be revoked for devices in the markets, those consumer devices would be useless. Even when revocation is limited to future devices, consumers could be precluded from purchasing new compatible products that could exchange or play back marked content with their legacy equipment.

Keeping these factors in mind, the Commission should craft a rule that permits revocation only after a clear demonstration of the following:

1. A breach is so widespread and significant that the DTV distribution platform has been compromised to such a point as to destroy its commercial viability, and the technology vendor has been unable to demonstrate that the breach can be adequately remedied; and
2. The harm to consumers and device manufacturers from revocation is outweighed by the harm to content providers and broadcasters of not revoking the authorization.

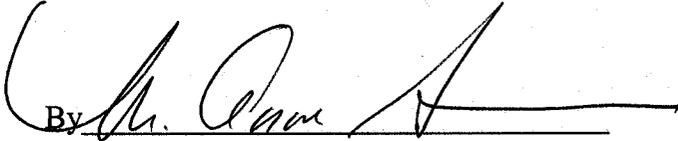
V. Conclusion

The DTV transition will be best advanced by the Commission's ensuring that the scope of the broadcast flag regime is defined as inhibiting the indiscriminate redistribution of DTV content over the Internet and declining to refine scope by reference to an inevitably ill-defined PDNE. In addition, the DTV transition will be furthered by implementing rules that establish functional and other criteria for digital content protection methods and allow vendor self-certification with an option for *bona fide* appeals to the FCC. The IT Coalition also urges the Commission not to unify the technology approval process in this proceeding with that established in the cable Plug & Play Proceeding. Finally, the Commission should not revoke content protection or recording technology in a manner that disables consumers' machines. Revocation should be used sparingly and only in those rare instances when the breach cannot be

repaired and the commercial viability of DTV as a delivery platform is destroyed, and harm to consumers and device manufacturers has been weighed against harm to content owners.

Respectfully submitted,

BUSINESS SOFTWARE ALLIANCE
COMPUTER SYSTEMS POLICY
PROJECT

By 

James M. Burger
M. Anne Swanson

of

Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W.
Suite 800
Washington, DC 20036
(202) 776-2534

Their Attorneys

February 13, 2004