BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

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

COMMENTS OF PHILIPS ELECTRONICS NORTH AMERICA CORPORATION ON FURTHER NOTICE OF PROPOSED RULEMAKING

Thomas B. Patton
Vice President, Government Relations
Philips Electronics North America Corporation
1300 Eye Street, N.W.
Suite 1070 East
Washington, D.C. 20005
(202) 962-8550

Rick Dorl
Vice President and General Counsel
Philips Consumer Electronics North America, a division of Philips Electronics North America Corporation
64 Perimeter Center, East
Atlanta, GA 30346
(770) 821-2232

February 13, 2004

Table of Contents

I. INTRODUCTION AND EXECUTIVE SUMMARY 1

II. STATEMENT OF INTEREST IN THIS PROCEEDING 4

III. THE OPEN PROCESS ESTABLISHED IN THE COMMISSION'S INTERIM APPROVAL RULES SHOULD BE EXTENDED PENDING A TRANSITION TO SELF-CERTIFICATION 5

A. The Commission's Interim Approval Rules Merit Application On a Longer-Term Basis 5

1. Approval of Digital Broadcast Content Protection and Recording Technologies Should Not Be Delegated, Formally or Effectively, To Any Single Industry or Self-Interested Private Parties 7

2. The Commission's Rules Should Permit, And The Commission Should Endeavor to Achieve, Approval of Multiple Technology Choices, Including Non-Encryption-Based Alternatives Such as Watermarking 8

B. Self-Certification Should Supplant the Interim Approval Rules As Soon As Warranted by Marketplace Conditions and Accumulated Experience 10

IV. THE APPROVAL OF DIGITAL BROADCAST CONTENT PROTECTION TECHNOLOGIES MUST BE BASED ON OBJECTIVE TECHNICAL CRITERIA AND REQUIRE REASONABLE AND NONDISCRIMINATORY LICENSING TO ACTUATE THE COMMISSION'S GOAL OF FOSTERING INNOVATION AND MARKETPLACE COMPETITION 12

A. Technical Criteria 13

1. Level of Security 14

a. Robustness of Components: The Ordinary User Standard 14

b. Vulnerability of Cryptographic Elements 15

c. System Security In Non-Encryption-Based Systems 16

2. Scope of Redistribution: Prevent the Unauthorized Indiscriminate Redistribution of Digital Broadcast Content Over the Internet 16

3. Authentication 18

4. Interoperability 19

5. Upgradability, Renewability and Revocation of Devices 20

B. Licensing Safeguards 22

1. Allowance of Approved Technologies Without Requiring Additional Approval 23

2. Prohibition on Reciprocal Non-Asserts 24

3. Changes 25

4. Prohibition Against Overreaching Compliance & Robustness Requirements 27

5. Nondiscrimination Between CE and IT Devices 28

V. IT IS IMPERATIVE THAT IMPOSITION OF THE BROADCAST FLAG REGIME NOT DEFEAT CONSUMERS' REASONABLE EXPECTATIONS FOR ENJOYMENT AND USE OF DIGITAL BROADCAST CONTENT 29

VI. REVOCATION OF A BROADCAST FLAG-TRIGGERED DIGITAL CONTENT PROTECTION TECHNOLOGY SHOULD BE DONE ONLY IN EXCEPTIONAL CIRCUMSTANCES AND NOT IMPAIR THE FUNCTIONALITY OF EXISTING EQUIPMENT 31

A. The Commission Should Adopt a High Threshold Standard for Determining If A Broadcast Flag-Triggered Technology Should Be Revoked 31

B. Failure Of A Content Protection System Must Do No Harm To Existing Consumer Products 32

VII. RELATIONSHIP BETWEEN THE BROADCAST FLAG AND PLUG AND PLAY PROCEEDINGS 33

VIII. CONCLUSION 34

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

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

COMMENTS OF
PHILIPS ELECTRONICS NORTH AMERICA CORPORATION

Philips Electronics North America Corporation ("Philips") respectfully submits these Comments in response to the Further Notice of Proposed Rulemaking in the above-captioned proceeding.[1]

I. INTRODUCTION AND EXECUTIVE SUMMARY

In its December 2, 2003 *Report and Order*, the Commission embraced certain core principles and established interim approval rules intended to ensure that the Broadcast Flag regulatory regime would: (1) lead to a competitive marketplace for digital content protection technologies; (2) not stifle competition and innovation in the consumer electronics and computer equipment markets; and (3) minimize adverse effects on consumers that would diminish their ability to enjoy expected uses of digital television content and products. The most important thing the Commission can do as a consequence of this *FNPRM* is to reaffirm, extend and, where appropriate, make permanent these principles and procedures. Any retreat from the pro-

[1] *Digital Broadcast Content Protection, MB Docket No. 02-230, Report and Order and Further Notice of ProposedRulemaking,*67 Fed. Reg. 53903 (December 2, 2003) ("*Report and Order*" and "*FNPRM*," as appropriate).

competitive, pro-consumer standards and safeguards adopted by the Commission would retard the DTV transition, precisely the opposite result the Commission seeks here.

In any order resulting from this *FNPRM*, the Commission must continue to ensure that, for the foreseeable future, the approval of digital content protection technologies for use with the Broadcast Flag is done by the Commission in an open and transparent process, with opportunity for public comment. Such approvals must be based on sound, objective, technical criteria and predicated upon licensing on reasonable and nondiscriminatory terms, conditions and prices. The Commission should establish a framework for making a transition to self-certification by proponents of digital content protection technologies once a competitive marketplace for digital content protection technologies exists and experience has confirmed the objective technical and licensing criteria to which it would be appropriate for manufacturers to self-certify. In no event should the Commission delegate approval determinations to one industry or a small group of companies with strong financial stakes in the outcome of the decision-making process.

Another important outcome of this *FNPRM* should be a more detailed and refined description of both the objective, technical criteria and the reasonable and nondiscriminatory licensing provisions and attendant safeguards necessary to achieve effective digital broadcast content protection while safeguarding competition and consumer expectations. While the *Report and Order* identifies certain "functional criteria," such as level of security, scope of redistribution, means of authentication, upgradability and renewability, etc., these really are areas of functional capability rather than technical criteria. What is required now is a judgment about which functions are important, how they should be grouped, and the development of standards by which they should be measured. In establishing such technical criteria and measurements, the Commission should provide sufficient flexibility to account for the architectural differences

between consumer electronics and computer equipment while simultaneously ensuring that its Broadcast Flag rules achieve functional regulatory parity between consumer electronics and computer equipment.

Similarly, the Commission should determine that certain license terms are simply incompatible with the reasonable and nondiscriminatory licensing policy established by the Commission. Examples of prohibited license terms would include provisions requiring licensees to give away (or "non-assert") their own intellectual property in order to obtain a license; change management provisions that deny licensees appropriate notice, opportunity for comment and dispute resolution; provisions granting technology sponsors the right to prohibit the use of other FCC-approved (and often competing) technologies; and, more generally, imposition of obligations on downstream devices beyond those required for covered demodulation products directly subject to the FCC rules. The establishment of specific licensing safeguards to give concrete expression to the Commission's policy of requiring reasonable and nondiscriminatory licensing is necessary to prevent anticompetitive conduct and to foster the open marketplace sought by the Commission.

Perhaps most importantly, in light of the Commission's objective of expediting the DTV transition, the Commission should ensure that imposition of the Broadcast Flag regime affords consumers the broadest possible opportunities to enjoy and use digital broadcast content consistent with the narrow goal of this regulation. To that end, the Commission should reaffirm that the appropriate scope of redistribution to be prevented is the "indiscriminate redistribution" of digital broadcast content over the Internet.[2] While the concept of a personal digital network environment ("PDNE") may be useful in ensuring certain baseline home networking capability

[2] *See Report and Order* at ¶ 10.

in this initial stage of digital broadcast content protection, the Commission should avoid enshrining the PDNE as a limitation on consumer use and enjoyment. The Commission's rules should encourage the development of digital content protection technologies that permit tailored, point-to-point Internet redistribution of digital broadcast content.

II. STATEMENT OF INTEREST IN THIS PROCEEDING

Philips has been and continues to be a global leader in digital television technologies and products and related consumer electronics products, including DVD players and recorders, personal video recorders, and Direct Broadcast Satellite systems. It is also a leader in video compression, storage and optical products, as well as in semiconductor technology.

Philips has been an active participant in the development of content protection technologies. Philips invented the Serial Copy Management System, or SCMS, preventing the unauthorized reproduction of multiple generations of copies of digital audio works from a copyright-protected original (while permitting a single generation of copies). Philips also is actively developing watermarking and fingerprinting technology to protect digital video and audio content.

Philips has been a constructive participant in inter-industry content protection activities, including the Copy Protection Technical Working Group (CPTWG), the Secure Digital Music Initiative (SDMI), the Broadcast Protection Discussion Group (BPDG) and, most recently, the Analog Reconversion Discussion Group (ARDG), co-chaired by one of Philips' most accomplished technologists.

Philips has been actively involved in this proceeding from its inception, endeavoring in its advocacy to ensure that a digital broadcast content protection regime addresses the legitimate concerns of the content community to safeguard their digital broadcasts from indiscriminate,

unauthorized redistribution over the Internet, while also preserving consumers' expectations regarding their use and enjoyment of digital broadcast content and promoting competition and innovation in the marketplace.

III. THE OPEN PROCESS ESTABLISHED IN THE COMMISSION'S INTERIM APPROVAL RULES SHOULD BE EXTENDED PENDING A TRANSITION TO SELF-CERTIFICATION

Philips commends the Commission, in tackling the enormous and complex task of establishing a digital content protection regime, for recognizing the paramount need to "formulate an open, objective approval process [for proposed digital content protection technologies]," and the essential role of such a process in "foster[ing] innovation and marketplace competition."[3] Indeed, the Commission's underlying goals of preserving the viability of free, over-the-air broadcasting and ensuring a successful transition to digital television,[4] are unattainable if, as a result of the Commission's actions in this proceeding, the marketplace for consumer electronics equipment used to access those services no longer offers consumers the same unparalleled choice it does today in terms of new technologies, flexibility, functionality and price.

A. <u>The Commission's Interim Approval Rules Merit Application On a Longer-Term Basis</u>

The Commission's rules for the selection of digital content protection and recording technologies on an interim basis ("Interim Approval rules"),[5] establish an open and transparent process for evaluating and approving competing content protection technologies, based upon

---

[3] *Id.* at ¶ 43.

[4] *See, e.g., Id.* at ¶¶ 4, 31.

[5] *See Id.* at ¶¶ 50-57; 47 C.F.R. § 73.9008.

objective, functional criteria.[6] They expressly take into account how such technologies will affect consumers' use and enjoyment of digital TV content.[7] They require that the technologies are licensed on fair, reasonable and nondiscriminatory terms.[8] The Commission makes these determinations, eliminating the threat of anticompetitive or anti-consumer conduct that could arise if a single industry or self-interested private parties controlled approval of those technologies.[9] The July 1, 2005 implementation deadline for these rules also reflects the Commission's long-standing recognition of the 18-month manufacturing cycle needed to implement new technologies in consumer electronics equipment.[10] The Commission provides all interested parties with an opportunity to comment on the proposed digital content protection technologies and affords proponents an opportunity to respond after which an expeditious Commission determination is rendered.[11]

In this *FNPRM*, the Commission asks whether and how such rules should be applied over the long term.[12] Philips urges that the Interim Approval rules, including refinements and clarifications to the requisite technical criteria and licensing safeguards, should govern the selection and approval of digital broadcast content protection technologies until such time as the Commission determines that a competitive marketplace for digital content protection

---

[6] *See Id.* at ¶ 55.

[7] *See Id.* at ¶ 55.

[8] *See Id.* at ¶ 55.

[9] *See Id.* at ¶ 52.

[10] *See Id.* at ¶ 57.

[11] *See Id.* at ¶ 54.

[12] *See FNPRM* at ¶¶ 61, 64.

technologies exists and sufficient experience has been gained applying technical and licensing criteria. Thereafter, the Commission should amend its rules to permit manufacturer self-certification based upon these same technical criteria and licensing safeguards.

1. Approval of Digital Broadcast Content Protection and Recording Technologies Should Not Be Delegated, Formally or Effectively, To Any Single Industry or Self-Interested Private Parties

Philips strongly commends the Commission, in the context of its Interim Approval rules, for recognizing the threat to competition posed by delegation of control over the approval of digital broadcast content protection and recording technologies to a single industry or a small group of self-interested private parties, rejecting that approach, and instead for reserving to itself digital broadcast content technology approval based upon objective criteria.[13] The Commission's stated concern "…with one industry segment exercising a significant degree of control over decisions regarding the approval and use of content protection and recording technologies in DTV-related equipment,"[14] is extremely well-founded, and one that must be guarded against with vigor. Indeed, as Commissioner Adelstein notes,

> [The Commission has] taken steps to assure that no single technology or set of companies is given a government endorsement to control all digital television reception and downstream distribution and recording. Our procedures ensure that no industry segment has veto power over the approval of technologies for use

[13] Philips had expressed these concerns in the initial phase of this proceeding. *See* In the Matter of Digital Broadcast Copy Protection, MB Docket No. 02-230, Comments of Philips Electronics North America Corporation (Dec. 6, 2003) ("*Philips Comments*") at 6, 22-23; *Id.,* Reply Comments of Philips Electronics North America Corporation (Feb. 19, 2003) ("*Philips Reply Comments*") at 27-30; *See also* September 23, 2003 Letter from Lawrence R. Sidman, on behalf of Philips Electronics North America Corporation, to Marlene Dortch in MB Docket No. 02-230 ("*Philips September 23, 2003 letter*") at 4 and Appendix B, Section Z.3, "Licensing Terms for Authorized Technologies;" October 21, 2003 Letter from Thomas B. Patton of Philips Electronics North America Corporation to Chairman Michael K. Powell in MB Docket No. 02-230 ("*Philips October 21, 2003 letter*"); October 22, 2003 Letter from Thomas B. Patton of Philips Electronics North America Corporation to Chairman Michael K. Powell in MB Docket No. 02-230 ("*Philips October 22, 2003 letter*")

[14] *Report and Order* at ¶ 52.

> with the flag. As we seek further comment on a long-term technology approval process, we have sought to establish interim procedures that are open and transparent. We have specified that the initial approval of technologies will be pursuant to functional requirements and a non-exhaustive list of objective criteria, without providing any entity a potentially dangerous first-mover advantage. Recognizing the steady convergence of computing and consumer electronics equipment in the home, our procedures are not intended to provide a regulatory advantage to anyone.[15]

There is no reason at this time for the Commission to retreat from the approach taken in its Interim Approval rules. That process, coupled with more fully articulated technological criteria and licensing safeguards, should be extended until a competitive marketplace for digital content protection technologies exists, mitigating the risks of first mover advantage or other effects that would impede competition or innovation. The Commission also will amass critical experience applying the Interim Approval rules, enabling it to determine a possible need for change. After the Commission approves multiple digital broadcast content protection technologies pursuant to the Interim Approval rules, and there is an opportunity to evaluate their effect on the marketplace, it would be appropriate for the Commission to revisit these rules, especially with a view toward moving to a true self-certification approach.

2. The Commission's Rules Should Permit, And The Commission Should Endeavor to Achieve, Approval of Multiple Technology Choices, Including Non-Encryption-Based Alternatives Such as Watermarking

The need to meet or exceed consumers' expectations regarding their use and enjoyment of digital broadcast content, as well as to protect competition and innovation in the digital content protection technology and equipment marketplaces, both underscore the importance of ensuring that manufacturers have a variety of alternatives – both with regard to output protection and recording protection technologies – from which to choose. Philips is heartened by the

[15] *Id.*, Statement of Commissioner Jonathan S. Adelstein.

Commission's stated expectation that it will approve "many different content protection and recording technologies, including but not limited to digital rights management, software-based, and non-encryption alternatives,"[16] and believes the Interim Approval rules adopted in this proceeding go a long way toward establishing a hospitable environment for the approval of multiple competing technologies.[17]

Particularly at the outset of this process, *i.e.,* before a competitive market has developed, it will be essential to mitigate, to the greatest extent possible, the potential for any single technology to receive, solely by virtue of a government mandate, a "first-mover" advantage over its erstwhile competitors. As Commissioner Copps stated upon the Commission's adoption of its *Report and Order*:

> If only one protection technology was to be available to consumers in the future, or if one technology was granted a first-mover advantage allowing it to entrench itself so firmly that new and better technologies are given no chance, we would have an intolerable result. Consumers would be forced to use a technology not because it provides consumer options or preserves fair use, but because they have no choice. Corporate interests would have trumped consumer interests. Reasonable uses of content by viewers could -- probably would -- be restricted, costs would rise and technology innovation would be hindered.[18]

In a perfect world, the Commission would safeguard against this evil by withholding approval of the first digital content protection technology until it is prepared to approve one or more competing technologies. Short of such guaranteed competition, the Commission, at a minimum, should structure its specific technical criteria so as not to limit or restrict different

---

[16] *Id.* at ¶ 10.

[17] Indeed, by providing for the selection of technologies in an open and transparent manner, and by expressly not conferring on any single industry actual or effective decisionmaking authority in the technology approval process, the Commission's Interim Process rules take a major step toward this goal.

[18] *Report and Order,* Statement of Commissioner Michael J. Copps.

types of digital broadcast content protection technologies, permitting encryption and non-encryption based systems, as well as DRM systems.

In that regard, Philips and other content protection technologists continue to believe that, ultimately, the protection sought by content owners – both for content traveling over digital and analog outputs – will most effectively, pervasively and affordably be achieved through a solution based on watermarking. Not only has no entity challenged this assertion, but watermarking has received support from the content community as a desirable alternative, or at least a complement, to encryption-based technologies, particularly given its ability to protect against indiscriminate redistribution of both (redigitized) analog and digital content. To encourage the availability of alternatives such as watermarking, fingerprinting and other innovative technologies for future implementation,[19] the Commission's technical criteria must be sufficiently flexible to permit their approval.

B. Self-Certification Should Supplant the Interim Approval Rules As Soon As Warranted by Marketplace Conditions and Accumulated Experience

Philips has long urged that the government should not be in the business of picking technology "winners and losers." Accordingly, Philips has supported an approach reliant upon self-certification (a concept embraced in several key legislative initiatives)[20] as a desirable means of enabling competitive and innovative digital content protection technologies to flourish, fulfilling the objective of content providers to prevent the unauthorized redistribution of digital broadcast content over the Internet to the public, and ensuring consumers have a wide array of

---

[19] *See Id.* at ¶¶ 25-26.

[20] *See*, *e.g.*, S. 1621 ("Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003"), 108th Cong. (2003); *see also,* House Energy and Commerce Committee Staff Discussion Draft, H.R. __ ("To require the Federal Communications Commission to take actions necessary to advance the transition to digital television service, and for other purposes"), (rel. Sept. 18, 2002).

choices. A self-certification approach need not and should not alter or undermine either the fundamental objective (*i.e.,* prevention of indiscriminate redistribution of digital broadcast content) or substantive requirements (*i.e.,* technical criteria and licensing safeguards) governing Broadcast Flag technologies. Rather, it would simply permit manufacturers, instead of the Commission, to certify that their digital broadcast content protection method, whether it be encryption, watermarking, digital rights management, software or other methods, achieves that objective and adheres to established objective, technical criteria and reasonable and nondiscriminatory licensing requirements. The Commission would retain the power to resolve complaints and impose sanctions if the certification proved false.

Philips believes that a regime permitting manufacturer self-certification should replace the Interim Approval rules as soon as marketplace conditions warrant. Self-certification should spur competition and innovation. It also would allow the Commission largely to extract itself from deep involvement in the digital content protection technology marketplace necessitated by the Interim Approval rules. At this time, however, it is difficult to predict how rapidly this shift to self-certification should or could occur. Much depends on whether the Interim Approval rules yield their intended pro-competitive results. Once a competitive market has developed and the Commission has amassed the requisite experience with how various approved content protection technologies are affecting the DTV transition, especially with regard to consumers, it would be appropriate for the Commission to seek comment on modifying its existing approval rules to permit self-certification.

IV. THE APPROVAL OF DIGITAL BROADCAST CONTENT PROTECTION TECHNOLOGIES MUST BE BASED ON OBJECTIVE TECHNICAL CRITERIA AND REQUIRE REASONABLE AND NONDISCRIMINATORY LICENSING TO ACTUATE THE COMMISSION'S GOAL OF FOSTERING INNOVATION AND MARKETPLACE COMPETITION.

The Commission's approval of any proposed digital content protection technology, particularly because it will be subject to a government mandate, must be based upon objective criteria. Establishing such clear, objective criteria would promote competition and innovation by making it easier to bring content protection technologies, and devices that employ them, to market, thus fostering a broader and increasingly more affordable array of consumer DTV devices – the lifeblood of the transition to DTV.

The Commission identifies a number of factors that it will consider when it evaluates technologies that are certified under its Interim Approval rules. The Commission divides these factors into four general categories: (a) technological factors; (b) licensing terms; (c) accommodation of consumers' use and enjoyment of unencrypted DTV content; and (d) "other relevant factors." The objective criteria defined in the Commission's final approval rules must address each of these categories.

Objective technical criteria are needed to ensure that an appropriate level of protection is provided by a technology, while at the same time maintaining a level playing field for all technologies. For example, the criteria should not favor consumer electronics equipment over computer products or vice versa. Consumer purchasing decisions should not be skewed by disparate regulatory treatment.

Reasonable and non-discriminatory licensing terms, including those governing the critical compliance and robustness rules that will extend the Commission's rules downstream from the Covered Demodulation Product, are needed for a number of reasons. First, in the "chain of obligations" model contemplated by the Broadcast Flag regulation, the downstream licensing

terms are a basic instrument of policy, ensuring that appropriate levels of protection, and concomitant restriction of consumer conduct, are applied. Second, if careful limits are not imposed, the licensing terms of approved technologies can harm, or even destroy, competition in content protection technologies. By granting a favored position to small groups of competitors, technology licensing terms also can harm competition among device manufacturers and restrict consumer choice and flexibility.

Standards or rules aimed at protecting consumers' use and enjoyment of the digital broadcast content, and the equipment they purchase to receive that content, are essential to ensure that consumers have sufficient confidence that their investment in digital television is one that will yield, as they expect, extraordinary advances in (and certainly no degradation of) the television experience they enjoy today.

A. Technical Criteria

In the *Report and Order*, the Commission identifies a number of "functional criteria" against which technologies should be evaluated, including level of security, scope of redistribution, authentication, upgradability, renewability, interoperability and revocability of compromised devices.[21] Philips observes that while each of these reflect a function or attribute of one or more security system architectures, they do not all necessarily apply to *every* architecture, and therefore should not be viewed as constituting an indivisible or complete set of criteria by which a technology should be judged. The principal benchmark against which any system must be judged is its efficacy at achieving the desired objective: namely, preventing the unauthorized, indiscriminate redistribution of broadcast content. That said, there are some areas of functionality, such as the level of security, that go to the heart of any digital content protection

[21] *See Report and Order* at ¶ 55.

system's acceptability for FCC approval, and for which an objective standard must be developed. Other areas, such as authentication, are suited only to encryption-based systems; therefore, the absence of such functionality in systems with alternative architectures should not result in a *prima facie* disqualification of those systems. Finally, other areas – notably upgradability, renewability and device revocation – are closely related (and raise similar issues), such that a technology's evaluation based upon each of these individual factors would be unnecessary and/or inappropriate. Below, Philips offers its views on the relative importance of each of these system attributes and, where feasible, suggests an objective standard by which it can be measured.

1. Level of Security

The concept of security of a digital broadcast content protection system, particularly encryption-based systems, encompasses two distinct components. The first is the physical construction of the components that are used to construct the system, essentially the robustness of the components. The second involves the vulnerability of the algorithms and protocols to attack. The robustness of components must be measured against the efforts and skills of the attacker, while the vulnerability of the basic cryptographic elements can be ascertained only by experience and mathematical analysis.

a. Robustness of Components: The Ordinary User Standard

Just as the Commission adopted an "ordinary user" robustness standard for Covered Demodulator Products in its Broadcast Flag regulations,[22] so too should it incorporate an "ordinary user" security standard in its evaluation of the robustness of digital broadcast content

[22] *See* 47 C.F.R. § 73.9007.

protection and recording technologies irrespective of a system's architecture. A few simple rules should be followed in implementing this standard:

First, it should be difficult for an average user to compromise the components of the Broadcast Flag copy protection system in any way that allows indiscriminate redistribution of broadcast content.

Second, it should be difficult for the expert to distribute any attack on a component in a form that is implementable by an average user. By an attack, we mean a method whereby the indiscriminate redistribution of broadcast content is enabled.[23]

Under such a standard, an approved system must be designed such that defeating or avoiding the technology would require the use of a device that is beyond the ordinary capability of an ordinary user to construct. Moreover, the distribution or use of a circumvention device which easily can be used by an ordinary user, also should be difficult. A detailed knowledge of the technology, or even the methods to defeat the system, should not, in and of itself, be sufficient to enable circumvention.

b. Vulnerability of Cryptographic Elements

Regarding the strength of encryption-based systems, the algorithm used should be published and not be vulnerable to a practical attack. Moreover, the key lengths should be sufficiently long to prevent attack by enumeration.[24]

---

[23] In the Plug and Play context, an "attack" also would extend to inappropriate copying of other marked content.

[24] For example, 56 bit keys can be attacked only by special purpose computers. Given the increasing speeds of computers and long life desired of these protection systems, 80 or 128 bit keys provide a preferable level of security.

Likewise, given the practical limitation on the robustness of components of the protection system, the loss of keys or other critical information from a single or small number of devices should not lead to the compromise of the entire protection system. Instead some method of rejection or revocation of these compromised elements should be available.

Known attacks against the cryptographic elements, or the system itself, should be considered and, to the extent possible, protected against. Where such attacks cannot be prevented, they should be made more difficult by effective combinations of available technology.

c. System Security In Non-Encryption-Based Systems

Although the Commission's Broadcast Flag rules currently are oriented toward encryption-based digital content protection technologies, the Commission should craft final rules to incorporate sufficient flexibility to provide an effective level of security through other means such as watermarking. Such alternative content protection technologies would necessarily have to be measured against different technical criteria to establish their effectiveness. The fundamental technical parameter remains the same: to prevent the indiscriminate redistribution of digital broadcast content. The establishment of specific measurements of meeting that standard in the case of non-encryption-based technologies should await the maturation of such technologies. It is critical, however, that nothing in the Commission's rules foreclose their development.

2. Scope of Redistribution: Prevent the Unauthorized Indiscriminate Redistribution of Digital Broadcast Content Over the Internet.

In the *FNPRM*, the Commission offers the appropriate standard that its rules should adopt dealing with scope of redistribution, namely that "a flag based system should prevent

indiscriminate redistribution of digital broadcast content."[25] This standard satisfies the core concern of content owners about the dangers of the "Napsterization" of their high-value broadcast content when transmitted in digital form. That concern formed the jurisdictional and logical basis for the Commission's decision.[26]

As the Commission itself recognizes, even ostensibly minimally intrusive content protection methods can prevent consumers from making permissible use of content.[27] Therefore, the Commission should afford the greatest flexibility for digital content protection technologies to evolve to permit broader consumer uses of digital content, not only within a so-called personal digital network environment ("PDNE"), however defined, but ultimately point-to-point retransmission over the Internet to a relative or close friend. Indeed, the utility of any content protection system in providing reasonable use of the content removes the inducement to defeat the system.

Under this standard, a digital content protection system that enables progressively greater consumer use and enjoyment of digital broadcast content should be viewed more favorably under the approval criteria, provided that it prevents the indiscriminate redistribution of such content over the Internet. There may well be utility to the Commission establishing parameters to describe a PDNE, including home networking, mobile applications and home-to-office links. The purpose of doing so, however, should be illustrative of permitted uses rather than to bound

---

[25] *FNPRM* at ¶ 63.

[26] *See Report and Order* at ¶¶ 8, 31.

[27] The Commission notes that the Broadcast Flag regime will diminish the functionality of legacy DVD players vis-à-vis their inability to playback digital broadcast content recorded on a broadcast flag-compliant device. *See Report and Order* at note 47.

permitted uses. The PDNE should not become a vehicle for limiting otherwise lawful consumer use of digital broadcast content.

Further, the Commission should not attempt to use the approval of technology to draw the bounds of copyright law or consumer fair use. These bounds cannot be drawn with sharp lines – fair use involves a fact-intensive, four-pronged analysis – and technological restrictions are likely to prohibit some transmissions that are lawful. The Broadcast Flag rulemaking was based on the specific, stated concern of "indiscriminate redistribution" of digital broadcast content, not a general need to adopt technology that will prohibit every transaction that might be deemed infringing. The courts exist for that purpose.

3. Authentication

It is important to note that not all digital content protection systems have architectures that employ authentication. For example, watermarking and fingerprinting (*i.e.,* forensic watermarking) have no need of authentication. Thus, this criterion is one of limited applicability, principally to encryption-based solutions. Philips urges the Commission's rules and its subsequent evaluation of all technologies take into account such architectural distinctions, applying functionally comparable criteria, so as not to inadvertently and unnecessarily prejudice the approval of certain classes of technologies.

In the case of encryption-based or other digital content protection and recording technologies that rely upon authentication, the technology should accomplish such authentication in a way that prevents non-authorized devices and revoked devices (or keys) from gaining access to protected material.

4. Interoperability

It is important to differentiate between technological interoperability and interoperability as a function of licensing. In the case of digital content protection technologies, technical interoperability requires only that the various rights states be understood and signaled or communicated from one device to another.

States in this context are the so-called "copy protection" state of the material. In the past, content has been labeled as being in four basic states: "Copy Never," "Copy Freely," "Copy Once" and "Copy No More."[28] The Broadcast Flag has introduced a new state: "Copy Freely But Do Not Redistribute Indiscriminately." Each protection system offered will have a technical method for describing or enunciating some or all of the five states described above.

In order to provide interoperability, it is essential that every approved Broadcast Flag protection system be able to translate its rendition of the appropriate state to any other approved system. A circumstance wherein one system combines several of these states into a single state, or places requirements on its rendition of this state which are different from those required by the Broadcast Flag regulation, would result in that system's not being interoperable with some or all of the other approved systems.

Technical interoperability is fundamental to the effective functioning of a digital content protection system. Thus, for a technology to be approved, it should be capable of signaling that content is redistribution-controlled content in a way that will allow the receiving device to use any other technology approved by the Commission.[29]

---

[28] For most purposes, the states "Copy No More" and "Copy Never" are redundant.

[29] *See* discussion at Section IV(B)(4), *infra.*

5. Upgradability, Renewability and Revocation of Devices

Although the *Report and Order* identifies these attributes separately, Philips believes that they should be considered together.

Upgradability should not be a mandatory technical criterion for an approved Broadcast Flag technology. While it may be a desirable feature in some implementations, those who have advocated inclusion of this criterion have not explained why it is necessary for a content protection technology that is subject to Commission review and approval. As a practical matter, security systems have major portions that cannot be upgraded (such as basic cryptographic algorithms). However, where a technology does permit some limited upgradability, any such upgrade should be subject to the same careful change management processes that the Commission applies to other modifications to ensure that all interests are protected. Specifically, the Commission should require that any such updates be implemented on a strictly forward-looking basis that permits users with existing technology to enjoy the full operation of equipment that employs the predecessor technology. The Commission also should require that it be made available on reasonable and non-discriminatory terms. Additionally, any change must be implemented in a manner that observes the long-recognized 18- to 24-month design and manufacturing cycle.

Rejection of compromised devices, or keys – an important capability often associated with renewability – historically and appropriately has been, and for many if not most security technologies will continue to be, accomplished through device revocation. Revocation of a device, or keys, is the responsive measure taken by a system owner to an attack by experts on the physical implementation of a system that has resulted in the compromise of that system's

security.[30] As discussed above, device revocation historically has been the means by which compromised security technologies are renewed. In so doing, however, and particularly in the context of ensuring consumer acceptance of DTV, it is essential that products (including interfaces) purchased in good faith by consumers retain their full functionality and usefulness for the lifetime of those products. Philips opposes any technology or interface revocation or retirement that might undermine consumers' good faith use of products they have purchased, or the home networks in which these products are used. To avoid such an outcome, any device revocation must be subject to strict limitations.

Specifically, an approved technology should be capable of permitting the revocation of a compromised device where such a compromise is found to be the result of a user's tampering or misconduct and where such revocation is possible without disabling similar or identical devices that have not been so compromised. Indeed, in a well-designed system,[31] compromise of a single device should never lead to the compromise of the entire system. The existing non-compromised equipment should continue to function even in the face of an attack on some of the devices in the hands of users. There should be no necessity for consumers to replace their hardware.

Software implementations that are distributed by the millions are a different manner. If a software implementation is compromised in a manner that is transferable to ordinary users, the entire implementation must be revoked *en masse*. No alternative exists: due to the fact that software almost always is distributed in identical form to all users, an attack on any single instance of software is an attack on *all* instances of that software. Typically, revocation

---

[30] In this regard, it is important not to confuse device revocation with technology revocation, *i.e.,* wherein the Commission revokes its approval of a technology for use with Covered Demodulator Products.

[31] *See* discussion regarding system security at Section IV(A)(1)(b), *supra.*

measures in such instances would be taken only after careful consideration and after an upgraded version of that software is made available to consumers.

B. Licensing Safeguards

Philips applauds the Commission's recognition of the need to ensure that technologies adopted pursuant to its digital content protection rules be licensed on "a reasonable and non-discriminatory basis."[32] As Philips has urged throughout this proceeding, the terms and conditions upon which digital content protection and recording technologies are licensed, including the critically important compliance and robustness rules that perpetuate the Commission's rules downstream, will play a crucial role in determining how and whether competition and innovation will develop and flourish in the technology and equipment marketplaces. The regime adopted by the Commission to implement the Broadcast Flag is a unique hybrid, combining a government technology mandate, with the full force and effect of law, together with reliance on a private license agreement which has the potential to confer enormous power on the licensor relative to other manufacturer licensees. In such a circumstance, the license needs to embody enforceable, pro-competitive safeguards, to avoid manipulation of government power to enforce self-serving decisions of private parties having the potential to reconfigure the competitive landscape to their own liking.

For that reason, Philips respectfully submits that the Commission should adopt a set of specific licensing safeguards where technologies are licensed to third parties to effectuate the general principle that licensing be on a reasonable and non-discriminatory basis. In some instances, such safeguards take the form of prohibitions of certain license terms which either are inappropriate to a government mandate, as is the case here, or carry with them such potential for

[32] *See Report and Order* at ¶ 55.

anticompetitive abuse that they should not be permitted, at least at this embryonic stage in the digital broadcast content protection technology marketplace. In other instances, these safeguards take the form of mandatory features of certain licensing terms without which the potential for anticompetitive conduct is so high as to be unacceptable.

1. Allowance of Approved Technologies Without Requiring Additional Approval.

The specification of technologies that may be used further downstream by a device that receives content from a covered product over an approved technology (from an approved output or by playing back an approved recording medium) has enormous potential for abuse and for destroying competition among content protection technologies. For example, the proprietor of an approved encryption technology that protects outputs may effectively kill competition by prohibiting the sink devices that decrypt the protected content from using a competing technology as an output from that sink device. Or, proprietors of families of technologies may favor particular output or recording technologies or prohibit the use of others.

Competition can be harmed not only by rejection but by delayed approval. Consider the following example: Suppose the FCC approves a single output protection technology that is compatible with downstream recording devices and approves two record protection technologies, each of which is designed for and used by competing recording formats. If the output technology has an independent ability to declare what record protection technologies its sink devices may use, or to delay the approval of one of the technologies, it can essentially determine the outcome of not only the competition among record protection technologies, but even the outcome of the format competition.

There is no reason for an approved technology to not allow the use of <u>any other approved technologies</u> in its sink devices. If a technology provides adequate security when it is used by a

directly covered demodulator product, it will provide adequate security for use by a downstream product. There is no question of incompatibility. Once the sink/playback device decrypts that content, it will know that the content is so protected, and should be able to route the content to any output or recording that is protected by a technology that the Commission has determined is suitable for such "redistribution-controlled" content.

To mitigate the potential for enormous competitive harm, the Commission, as a condition of its approval of a digital content protection technology, should require that an approved output or recording technology allow use of digital outputs and recordable media protected by other approved technologies without requiring additional approval. A license provision providing to the contrary would have to be deleted to gain Commission approval of the digital content protection technology.[33]

2. Prohibition on Reciprocal Non-Asserts

In the context of a government mandate, as is the case here, the notion that a licensor could compel a licensee to acquiesce in the confiscation of intellectual property it may have in the system as a condition of licensing the government-approved technology is inherently abusive. In the unique context of digital content protection, it also is perverse, requiring a licensee to surrender its intellectual property to enable a content provider to protect its intellectual property. Such reciprocal non-assert provisions discriminate invidiously against licensee/manufacturers who have intellectual property in the system over those who do not. Recognition of the inappropriateness of a reciprocal licensee non-assert provision in this type of license – suffused with government involvement – is not unprecedented. The DFAST license

[33] As discussed *supra,* under no circumstances should the Commission establish a regime wherein a self-interested party is given *carte blanche* to change its technology or technologies, or the associated licensing terms and conditions, after receiving the initial approval.

embodied in the "Plug and Play" regime approved by the Commission for unidirectional cable-ready products imposes on licensees a reasonable and nondiscriminatory (RAND) licensing obligation as opposed to a reciprocal licensee non-assert.[34]

The Commission should adopt a specific licensing safeguard, prohibiting the use of reciprocal licensee non-asserts if a proponent seeks to obtain Commission approval of its systems. Thus, the licensing terms and conditions associated with an approved technology shall not require licensees to agree not to assert any intellectual property they may have in the technology as a condition for obtaining a license, but such terms may require licensee patents to be licensed on reasonable and nondiscriminatory terms.

3. Changes

As discussed in detail in prior Philips filings in this proceeding,[35] the ability of a licensor to impose changes unilaterally without notice or opportunity for licensee input has the potential to confer enormous competitive advantage regarding product development and lead time to market. Privately negotiated and coercively imposed changes could be more or less restrictive than provided under current versions of the licenses, in either case creating the potential for anticompetitive effects.

Absent open and fair change management procedures, there would be nothing to assure that copy limitations, restrictions on digital and analog outputs, limitations on PVR processing, and other rules won't be imposed by fiat. By virtue of their licenses with associated approval rights for changes and compliance and robustness rules, licensors would be positioned to exercise unlawful market power to restrain competition in the digital content protection

---

[34] *See* DFAST license at ¶ 3.5.

[35] *See* Philips Reply Comments at 28-29; Philips October 22, 2003 letter at 6-8.

technology market and to leverage that advantage into adjacent markets for consumer electronics products themselves. They would have advance, inside information, affording them substantial lead time to market and other competitive advantages in their investments, business strategies, and product design. One likely area where this arrangement would stifle innovation and raise the spectre of leveraging market power in digital content protection technologies into a competitive advantage in consumer electronics product design is in the area of manipulation, organization, processing and storage of digital content.

Once again, the DFAST license used in the Plug and Play agreement is instructive. Paragraph 6.2 of the DFAST license, provides for a change management procedure for certain changes to the Compliance and Robustness rules. The DFAST change management process moves in the right direction; the Commission's rules should go farther. They should address the lead-time to market advantage that may be gained by permissive changes that broaden licensee rights, as well as address changes in the underlying technology. The Commission should require similar change management procedures in any license accompanying a candidate digital content protection technology. The licensing terms and conditions associated with an approved technology should require a fair and open change management procedure applicable to any material change in the technical specifications, compliance and robustness rules,[36] providing for prompt notice of contemplated changes, opportunity for licensees and content providers to comment upon and reconcile their differences regarding any such changes before they are implemented, disputes resolution procedures, either before the Commission or in an arbitration,

[36] Concerns regarding changes in compliance and robustness rules will be largely ameliorated under the proposals discussed in Sections IV(B)(1) and IV(B)(4).

and finally a reasonable time in which to implement changes consistent with the manufacturing cycle of the industry.

4. Prohibition Against Overreaching Compliance & Robustness Requirements

The compliance rules adopted by the Commission set out the framework for what is necessary to protect broadcast content from Internet redistribution. They are the only rules that apply to covered demodulator products, which can be almost any product in the content chain in the home. The same can be said for the security, or "robustness," standard adopted by the Commission, which requires that content protection be implemented "in a reasonable method so that they cannot be defeated or circumvented merely by an ordinary user using generally-available tools or equipment."[37] These rules have been determined by the Commission to be the rules necessary to protect broadcast content. It is not rational to impose higher standards on downstream devices. It is well known that the level of security provided by a system is equal to the security provided by the weakest link in that system. Higher downstream standards thus will not add to the level of security provided to broadcast content; it will only add cost and complexity.

During the initial phase of this proceeding, proponents of some technologies argued that because their technology can be used for other "redistribution controlled" content (*e.g.*, EPN content) that could not be distinguished from Broadcast Flag content, this limitation was not appropriate. That argument makes no sense. There is no justification for treating other "redistribution-controlled" content any differently than broadcast content. The whole purpose of the Broadcast Flag rulemaking was to level the redistribution control playing field between

[37] 47 C.F.R. § 73.9007.

broadcast and other content. The Broadcast Flag rule establishes the appropriate level of protection for redistribution control. If a system wishes to provide a different type of redistribution control for other content, it should establish a distinct state to identify such content.

Thus, the Commission should establish the following license safeguard: The licensing terms and conditions associated with an approved technology shall not obligate devices that receive or play back digital broadcast television content using such technology to conform to compliance and robustness rules that exceed or differ from those applicable to devices directly subject to the compliance and robustness rules set by the Commission.

5. Nondiscrimination Between CE and IT Devices

Except where unavoidable due to inherent differences in system architecture or design, the licensing terms and conditions associated with an approved technology should apply equally and without discrimination, in either applicability or effect, to both consumer electronics and IT devices.

This principle of nondiscrimination addresses a different potential problem than those discussed above. Increasingly, in the digital television product environment, consumer electronics and computer equipment are going to be direct competitors. Differential licensing terms have the potential to skew consumer purchasing decisions in favor of one class of devices over another. In the past, there has been an attempt to exempt computers from certain obligations. Yet, there is no rational basis to impose more stringent standards on consumer electronic devices, particularly where the greatest concern about unauthorized, indiscriminate redistribution of digital broadcast content over the Internet arises in the computer environment.

V. IT IS IMPERATIVE THAT IMPOSITION OF THE BROADCAST FLAG REGIME NOT DEFEAT CONSUMERS' REASONABLE EXPECTATIONS FOR ENJOYMENT AND USE OF DIGITAL BROADCAST CONTENT

Philips concurs wholeheartedly with the Commission's finding that advancing the DTV transition requires striking a "delicate balance [between assuring] the availability of high value digital content to consumers in a secure, protected format…and [preserving]…consumers' ability to enjoy programming when and where they choose."[38] That the Commission has determined to mandate the use of certain approved technologies to address content owners' concerns, on the one hand, must be counterbalanced by ensuring that the technologies it does approve for that purpose facilitate consumers' enhanced enjoyment of and interaction with over-the-air content – and allow them to experience the tremendous benefits promised by the transition to digital television. Limitations on consumers' ability to use and manipulate DTV that exceed those applied today to analog television risk slowing the DTV transition. Conversely, the transition will move far more smoothly and rapidly if the great flexibility of digital technology is allowed to enhance the consumer experience by facilitating storage, processing, organization and handling of content.

As discussed above in connection with the elaboration of the scope of redistribution technical criterion, perhaps the most important action the Commission can take in this phase of the proceeding to protect consumers' use and enjoyment expectation is to reaffirm the core limitation on the Broadcast Flag regime: *i.e.,* that its purpose and effect is to prevent the unauthorized "indiscriminate redistribution" of digital broadcast content over the Internet.[39]

---

[38] *Report and Order* at ¶ 1.

[39] *See FNPRM* at ¶ 63.

Under this formulation, all other lawful uses of such content by consumers should not be abridged by the Broadcast Flag regime.

In endorsing this standard put forward by the Commission, Philips is not suggesting that a digital content protection technology must permit tailored and lawful point-to-point redistribution over the Internet in order to be approved by the Commission at this time. Philips is keenly aware of the current technological limitations that render it difficult to prevent indiscriminate redistribution today without also effectively precluding any Internet redistribution. What is critical for consumers, however, is that the Commission's rules not enshrine today's technological limitations but, to the contrary, create incentives for technological innovation that will prevent indiscriminate redistribution but permit other targeted, lawful Internet redistribution of digital broadcast content, such as from one's home to one's office. At some future time, when technology has advanced, the Commission may well want to revisit this standard and require that new digital content protection technologies provide this capability as a condition of approval.

Within this context, Philips believes that the concept of a personal digital network environment ("PDNE") may be helpful in providing some benchmarks for consumer expectations about uses that will be clearly permitted in the presence of the Broadcast Flag once technology enables such uses. These would include redistribution of digital broadcast content:

- Between and among all devices in the home;
- To personal portable devices (such as a PDA, laptop computer or mobile phone);
- To one's motor vehicle or boat; and
- Between an individual's primary and secondary residences, and between one's home and office.

Philips cautions, however, against engrafting a PDNE into the Broadcast Flag regulations at this time because of the very real danger that the PDNE may become a limitation on consumer use rather than an enabler of consumer use.

VI. REVOCATION OF A BROADCAST FLAG-TRIGGERED DIGITAL CONTENT PROTECTION TECHNOLOGY SHOULD BE DONE ONLY IN EXCEPTIONAL CIRCUMSTANCES AND NOT IMPAIR THE FUNCTIONALITY OF EXISTING EQUIPMENT

It is axiomatic that content protection technologies, no matter how "bulletproof" they may appear, inevitably are susceptible to being compromised. Indeed, for every new content protection technology developed, legions of "hackers" are ready to pit themselves against that system. Technologies approved for use with the Broadcast Flag will be no exception. In that regard, the question, therefore, is not "whether" a Broadcast Flag-triggered technology will be compromised, it's "when" and, most importantly, "what next" – *i.e.*, what will be the consequences, both for the content and consumers, when a system is compromised, and, especially, if such a compromise merits revocation of that technology? Indeed, while revocation is a necessary and legitimate tool for "weeding out" digital content protection technologies that have been compromised, given the unavoidable cost ramifications (for manufacturers and possibly consumers), it is a tool that must be wielded only under extraordinary circumstances, and then with great care. To address these concerns, Philips offers several suggestions as to the standard for determining whether a technology should be revoked and the mechanisms for executing such a revocation.

A. <u>The Commission Should Adopt a High Threshold Standard for Determining If A Broadcast Flag-Triggered Technology Should Be Revoked</u>

Philips urges the Commission to adopt a high-threshold standard for the revocation of digital content protection technologies in this proceeding. Specifically, revocation of a

Broadcast Flag-triggered digital content protection technology that results in that technology's removal from the list of Commission-approved technologies should only occur upon a showing that the compromise is significant and widespread and cannot be repaired via device revocation or other renewability methods. Moreover, such revocation should not occur unless and until there is a suitable replacement technology available. Importantly, and consistent with the historic and consistently-recognized design and manufacturing cycle for integration of new technologies, device manufacturers must be allowed 18 to 24 months to implement the replacement technology.[40]

By contrast, a more lenient standard for revocation discussed in the *FNPRM, i.e.,* that the compromise be merely "perceived to be insecure,"[41] is unacceptably vague, so much so that it would likely lead to enormous uncertainty in, if not outright abuse of, the revocation process.

B. Failure Of A Content Protection System Must Do No Harm To Existing Consumer Products

It is essential to the continued and complete acceptance of DTV by consumers that the Commission adopt a technology revocation mechanism that ensures that compliant digital equipment purchased by consumers and legitimately obtained digital content are not subject to any loss of functionality as a result of a digital content protection technology's revocation. Indeed, there is perhaps no greater nightmare scenario – nor any greater threat to DTV's acceptance by consumers – than that wherein consumers find that their lawfully obtained, erstwhile compliant, digital equipment, and the digital content obtained with that equipment, no

[40] Of course, the licensing terms and conditions of any replacement technology would be subject to Commission scrutiny for being reasonable and non-discriminatory.

[41] *FNPRM* at ¶ 65.

longer is capable of functioning in the manner for which it was purchased. A requirement that consumers (somehow) retrofit their equipment would be equally unacceptable.

Philips therefore urges the Commission to adopt mechanisms for digital content protection technology revocation only where the need for such action is clearly justified and then only on a going-forward basis, preserving the full functionality of existing devices.

VII. RELATIONSHIP BETWEEN THE BROADCAST FLAG AND PLUG AND PLAY PROCEEDINGS

In its *FNPRM*, the Commission seeks comment on whether a unified regime should be employed governing the standards and procedures for approval of digital content protection technologies in the Plug and Play and Broadcast Flag contexts.[42] Philips does not believe that a "unitary" regulatory regime is required to govern both Plug and Play and the Broadcast Flag because of the fundamental differences in the origins and purposes of these proceedings. Philips would observe that much of the impetus for "coupling" these proceedings arose out of the forceful advocacy of the content community to impose both sets of regulations at the same time, an issue since resolved by the *Report and Order*. That timing issue is unrelated to the substantive similarities or differences between the two sets of regulations.

In one very important substantive respect, however, Commission action in discharging its regulatory obligations to approve digital content protection technologies under the Broadcast Flag regulations should be presumptively binding upon CableLabs in discharging comparable functions in the Plug and Play context. Where the Commission approves a technology under the Broadcast flag regime, it should be incumbent upon CableLabs, as a general matter, also to approve that technology under the Plug and Play rules. As indicated above, most digital content

[42] *See FNPRM* at ¶ 61.

protection technologies submitted to the Commission for Broadcast Flag purposes will be broader in scope and also encompass copy control functions for non-broadcast content. Moreover, "boxes" will be designed and manufactured to fulfill both functions. Unless CableLabs were able to meet a very heavy burden of proof to demonstrate that functions associated with copy control not present in the Broadcast Flag context could justify rejection where the Commission had approved a digital content protection technology for use with the Broadcast Flag, CableLabs should be required to approve it as well under the DFAST license. The same is true for the converse situation where the Commission rejects a technology.

The presumptively binding nature of Commission action on CableLabs should unquestionably extend to Commission judgments regarding the propriety of specific terms and conditions contained in the licenses for digital content protection technologies. To the extent the Commission concludes, for example, that a non-assert obligation is incompatible with reasonable and non-discriminatory licensing under the Broadcast Flag rules, that restriction should be imported into technology licenses under the Plug and Play regime. Such judgments reflect fundamental public policy determinations about licensing, and there is no basis for concluding that different considerations should apply to such questions in the Plug and Play context from those that apply in the Broadcast Flag context.

VIII. CONCLUSION

Although the Commission has taken very important first steps to enhance the prospects that the Broadcast Flag regulatory regime will not lead to a host of anticompetitive, anti-consumer problems that surely would impede rather than accelerate the successful DTV transition, the Commission's work in this new area of regulation is only beginning. At this very early stage – *i.e.*, preceding actual deployment of digital content protection technologies to

prevent the unauthorized, indiscriminate redistribution of digital broadcast content – it is critical that the Commission, in the further rules it may adopt as a result of this *FNPRM*, and in its technology approval process, be aggressive in promoting a competitive and innovative marketplace. Of particular importance to that objective is ensuring that one industry segment does not obtain an informal veto over selection of digital content protection technologies. Equally important, the Commission must amplify on the principle of reasonable and non-discriminatory licensing by providing guidance that specific types of licensing provisions are unacceptable within the context of a government mandated system and will preclude approval of the technologies.

Respectfully submitted,

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION

Thomas B. Patton
Vice President, Government Relations
Philips Electronics North America Corp.
1300 Eye Street, N.W.
Suite 1070 East
Washington, D.C. 20005
(202) 962-8550

Rick Dorl
Vice President and General Counsel
Philips Consumer Electronics North America, a division of Philips Electronics North America Corporation
64 Perimeter Center, East
Atlanta, GA 30346
(770) 821-2232

February 13, 2004