

TABLE OF CONTENTS

	Page
SUMMARY	i
I. INTRODUCTION	2
II. SIGNAL SECURITY CANNOT BE SACRIFICED TO ACHIEVE COMMERCIAL AVAILABILITY OF NAVIGATION DEVICES	7
A. Separation of Security and Non-Security Functions	11
B. Protection Against Unauthorized Copying	13
C. No "Right to Attach" Should Apply to Devices Used or Useful to Facilitate Unauthorized Reception	14
III. EQUIPMENT AND ENTITIES COVERED BY SECTION 629	18
A. Equipment Covered	18
B. Entities Covered	22
IV. COMMERCIAL AVAILABILITY	26
A. Definition of Commercial Availability	27
B. Preference for Marketplace Solutions	28
C. Integration of Navigation and Security Functions	30
D. Separation Between MVPDs and Retail Outlets	31
V. PORTABILITY AND INTEROPERABILITY	32
A. Distinction Between Analog and Digital Equipment	34
B. Development of Digital Architecture to Promote Portability and Interoperability ..	36
VI. PREREQUISITES FOR "CABLE READY" DIGITAL NAVIGATION DEVICES	39
VII. SUBSIDIZATION OF HARDWARE BY PROGRAMMING SERVICE FEES	43
VIII. DEVELOPMENTAL WAIVERS	45
IX. ALL RULES ADOPTED PURSUANT TO SECTION 629 SHOULD SUNSET ON A NATIONAL BASIS	47
X. CONCLUSION	49

SUMMARY

Time Warner supports the Commission's efforts to assure the commercial availability of "navigation devices" used by consumers to access the services provided by MVPDs. Fostering competition in the manufacture and sale of navigation devices used to receive multichannel video programming services will maximize the utility of MVPD broadband networks, ultimately benefitting both consumers and the industry. However, the Commission's similar experiences in the telephone equipment context would be an inappropriate model on which to base the regulatory treatment of equipment used with broadband MVPD distribution systems. Broadband MVPD distribution systems utilize a radically different network architecture and offer an entirely different type of service than that used or offered by narrowband telephone networks. Moreover, the unbundling of services and equipment raises significant security concerns unique to the MVPD context. These concerns strongly militate in favor of the development of a new model that fully takes into account the unique characteristics associated with and problems encountered by broadband MVPD distribution systems.

For example, protection of signal security must be a predominant consideration. If MVPDs are hampered in their ability to protect the integrity of their networks, and indeed their businesses, competition and consumers will be harmed in the long run. The Commission must first take care to ensure that the navigation devices which are to be made commercially available are not defined to include equipment which performs security functions. Second, due to the differing technologies utilized by different categories of MVPDs, and the unique security concerns of each particular system, each MVPD must be allowed to establish technical standards and specification for navigation equipment that can be used on its system. Finally, the Commission must make its equipment authorization process more stringent as it relates to obtaining approval for cable system terminal devices.

Specifically, the Commission should revamp its CSTD authorization process by requiring applicants to make more detailed demonstrations of the technical and marketing steps taken to prevent unauthorized access to MVPD networks and services. The Commission should also provide for a period of time (60 days) between authorization grant and marketing so that interested parties have an opportunity to scrutinize the new device and raise objections if such safeguards are inadequate, as well as adopting a presumption that companies shown to have been involved in any unlawful MVPD descrambling activity may not obtain future authorizations for their devices. Each of these steps would greatly assist the Commission and the industry in ensuring that the CSTD authorization process is not misused to validate pirate equipment.

In addition, the rights of copyright holders must be protected. The Commission must recognize that the availability of powerful yet inexpensive computers which can be programmed to emulate any kind of consumer electronics, coupled with the fact that it is possible to make an unlimited number of unauthorized perfect copies from a single authorized digital source, dramatically increases the consequences of piracy and copyright infringement by several orders of magnitude. Accordingly, any digital video navigation device that is commercially available must either be equipped with proper security to prevent digital signals from being delivered in the clear at the output of the device, or utilize an appropriate interface that will prevent unauthorized copying and piracy.

Accordingly, the term "navigation device" for purposes of Section 629 should not encompass any device which provides any security or conditional authorization function, but rather should be strictly limited to devices which add features or functionalities to any service which a consumer has been expressly authorized to receive from an MVPD. Thus, any

equipment that performs network security functions, such as decoders, descramblers, addressable converters, network interface modules, interdiction devices, and any other equipment performing security functions, must be excluded from the scope of this proceeding. Furthermore, as such equipment should not limit subscribers' ability to receive MVPD services of their choice, any commercially available video navigation device which is marketed as "cable ready" must be able to support all functions and services offered by a cable operator (*e.g.*, on-screen guides, impulse pay-per-view, *etc.*).

Section 629 should cover a wide range of video distribution systems, *including, but not limited to*, cable television systems, high and medium power DBS and satellite service systems (C-band, Ku band FSS, and Ku band BSS), satellite master antenna systems, wireless cable systems (*e.g.*, multichannel multipoint distribution service, instructional television fixed service, and local multipoint distribution service), multichannel digital television broadcast stations, and open video systems. All of these entities provide paying subscribers with "multiple channels of video programming," thus falling within the express definition of a MVPD under the statute.

As long as a subscriber can purchase or lease a compatible navigation device from any single unaffiliated manufacturer, retailer, or vendor who is licensed to distribute that equipment, such devices should be deemed commercially available. Substantial flexibility should be used in determining whether the commercial availability standard has been satisfied. The Commission should not involve itself in making judgments as to the most efficient way to market devices to consumers. The marketplace, not the Commission, can best respond to consumer demand for MVPD compatible video navigation devices and dictate the number of outlets in any particular community and the most efficient marketing structure.

Because of the large embedded base of analog video navigation devices, as well as integrated navigation/security devices, the Commission should not prohibit MVPDs from continuing to offer integrated converter/descramblers. Consumers should not be forced to shoulder the burden of having the substantial investment in perfectly serviceable equipment made obsolete by regulatory fiat. As long as consumers have the *option* to purchase or lease component navigation devices, there is no reason they should not also have the option to obtain an integrated navigation/security devices from their MVPD.

In attempting to promote portability and interoperability, the Commission must distinguish between analog and digital video navigation devices. There is already a large base of analog navigation devices currently in use by various MVPDs. While many such devices are neither portable nor interoperable, they are nonetheless completely functional and serviceable and there is simply no justification to require that such devices be replaced prior to the end of their useful life. A similar degree of deployment does not yet exist in the digital environment, thereby presenting a more promising opportunity to achieve a greater degree of portability and interoperability than will be possible with analog distribution technologies.

There are natural incentives within the industry to develop a common basic architecture which promotes the portability and interoperability of digital navigation devices, as evidenced by the many private sector initiatives which have already taken place. The development of industry standards regarding a common basic digital navigation platform must be robust enough to support various MVPD services as well as third-party ancillary services delivered on a competitive basis, and must be adaptable in the digital context without compromising MVPD network security and intellectual property concerns. Indeed, such a common architecture, supporting a hardware transparent addressable applications

environment, must be flexible enough to support a multiplicity of applications, both present and future, obtained from a variety of sources. This would be greatly facilitated through the use of a common executable programming language, such as HTML, compatible across different operating systems.

Time Warner believes certain basic prerequisites which are necessary for any digital equipment that is intended to be marketed commercially as "cable ready" for use with cable television systems. First, security functions must be removable and replaceable in the event that security is compromised. Second, the equipment must be designed to ensure that copy protection mechanisms cannot be bypassed or defeated. Third, the equipment must contain a sufficiently robust hardware platform to support the downloading and execution of various applications, such as program guides, on screen displays, and impulse pay per view that may differ among MVPDs or be provided by multiple vendors over a single MVPD.

The offering of navigation devices at discounted prices by MVPDs is ultimately pro-consumer. Equipment discounts should only be a concern where they are not real discounts, but rather where the cost of the equipment is hidden in a long term programming service agreement. If DBS providers and certain other MVPDs are allowed to continue to link equipment discounts to long-term service contracts, there is no rational basis for not allowing all MVPDs to have the same flexibility.

Again, Time Warner whole-heartedly supports the goals behind fostering competition in the manufacture and sale of MVPD navigation devices, but insists that the Commission not discount unique security concerns associated with MVPD equipment, and that industry organizations be given a full opportunity to develop solutions to these complex issues before the government intercedes.

BEFORE THE
Federal Communications Commission

WASHINGTON, D.C. 20554

In the Matter of)
)
Implementation of Section 304 of the)
Telecommunications Act of 1996) CS Docket No. 97-80
)
Commercial Availability of)
Navigation Devices)

COMMENTS OF TIME WARNER ENTERTAINMENT COMPANY, L.P.

Time Warner Entertainment Company, L.P. ("Time Warner"), by its attorneys, submits these comments in response to the above-captioned Notice of Proposed Rulemaking released by the Federal Communications Commission ("FCC" or "Commission") on February 20, 1997.^{1/} Time Warner is a partnership, which is primarily owned (through subsidiaries) and fully managed by Time Warner Inc., a publicly traded Delaware corporation. Time Warner is comprised principally of three unincorporated divisions: Time Warner Cable, the second largest operator of cable systems nationwide; Home Box Office, which operates pay television programming services; and Warner Bros., which is a major producer of theatrical motion pictures and television programs. In addition, an affiliate of Time Warner holds an interest in a direct-to-home satellite programming service provider. Accordingly, Time Warner would be directly affected by any regulations which the Commission ultimately adopts to implement Section 304 of the 1996 Telecommunications Act.

^{1/}Notice of Proposed Rulemaking, CS Docket No.97-80, 62 Fed. Reg. 10011 (rel. February 20, 1997) ("NPRM").

I. INTRODUCTION.

Time Warner supports the Commission's efforts to implement Section 304 of the 1996 Telecommunication Act which requires it to assure the commercial availability of "navigation devices" used by consumers to access the services provided by multichannel video programming distributors ("MVPDs").^{2/} This is a daunting task. Technology is advancing at a dizzying pace and competition continues to increase for the services offered by terrestrial and satellite based MVPDs. These MVPDs utilize different delivery technologies, different modulation schemes, have different bandwidth requirements, and operate in different portions of the frequency spectrum. Some MVPDs are fully analog, some are fully digital, while others provide a mix of analog and digital services. As a result, equipment requirements can vary dramatically among different classes of MVPDs and, to a lesser degree, among MVPDs of the same type. Additionally, new equipment is being developed and deployed almost daily to support new services and offer a richer variety of functions and features. Older equipment is in danger of becoming outmoded and obsolete if it cannot be upgraded.

In its NPRM, the Commission proposes to use its experience with unbundling equipment and services in the telephone context as a starting point to develop a regulatory model for fostering the retail availability of navigation devices used to access multichannel video programming services and other services offered by MVPDs.^{3/} This proposal should be rejected. Telephony is a particularly inappropriate model on which to base the regulatory treatment of equipment that is intended for use with broadband video distribution systems.

^{2/}Section 304 of the 1996 Telecommunications Act added Section 629 to the Communications Act of 1934.

^{3/}NPRM at ¶¶ 8-10.

The Commission itself notes that the uniformity of telephone technology, equipment, and connectivity arises from the fact that for most of its history, the telephone industry was a monolithic, national monopoly created by, and supported by, industry-wide regulation.^{4/} This stands in stark contrast with the development of various multichannel video programming service technologies which utilize a variety of transmission and security techniques and which have often developed on a balkanized, community-by-community basis.

The Commission's experience in requiring the unbundling of equipment from service in the telephone context is only marginally useful in implementing Section 629. Broadband cable television distribution systems utilize a radically different network architecture than the centralized switched star configuration traditionally employed by narrowband telephone networks and cable systems offer a fundamentally different service than that offered by telephone systems. With its tree and branch architecture, cable television signal routing and security functions are often accomplished at or near the subscriber's premises, whereas in the telephone model, such functions are normally accomplished at the telephone company's central office. Simply put, the commercial availability of certain types of equipment located on or near the customer's premises raises significant security concerns in the cable television context that are not present in the telephone context. The lack of uniform broadband transmission standards and the need to protect signal security and network integrity inherent in cable television architecture and service strongly militate in favor of the development of a new model that fully takes into account the unique characteristics associated with and problems encountered by broadband cable television distribution systems.

^{4/}NPRM at ¶ 10.

As the Commission adopts regulations to cover equipment falling within the scope of its "navigation device" definition, it should be mindful of important differences between analog and digital video navigation devices. Unlike digital navigation devices, analog devices enjoy a sizable embedded base, but that base can be expected to diminish over time as MVPDs convert their networks to digital transmission. Digital transmission presents many unique and complex problems not shared with analog distribution, and the Commission must tread carefully to guard against imposing untested interoperability and portability requirements that are not marketplace driven and which could stifle innovation and pose undue security risks. The significant progress made through cooperative interindustry efforts in this "dawn" of the digital era exhibits great promise to avoid the incompatibility problems that arose and which had to be overcome in the world of analog MVPD service delivery. The Commission should strongly encourage the affected industries to continue to work together to develop marketplace solutions to very complicated and difficult issues and should intervene only when necessary to ensure continued progress toward achieving the goals of Section 629.

A model for such problem solving already exists and has been followed in adopting decoder interface regulations applicable to analog devices in connection with the implementation of the equipment compatibility provisions of the 1992 Cable Act. The work of the Cable-Consumer Electronics Compatibility Advisory Group ("C3AG") represents a practical solution for furthering Congress' desire to make navigation devices commercially available by allowing security functions to be completely removed from analog navigation devices. This work also represents a good starting point for accomplishing the same eventual

result for digital navigation devices, but much additional effort is needed.^{5/} The cable, computer and consumer electronics industries should be encouraged to continue to work together to develop specifications for a renewable security system and a hardware platform that will support an environment that will allow applications to be downloaded and executed to support features and services, such as program guides and other on screen displays, on a hardware transparent basis. The Commission must also support a requirement that any digital equipment offered competitively either be equipped with the proper security to prevent digital signals from being delivered in the clear at the output of the device, or utilize an industry established protocol that will prevent unauthorized copying and piracy.

The FCC can greatly facilitate ongoing inter-industry efforts to increase portability and interoperability of video navigation devices over the long term and allow a retail market for such equipment to develop through open competition. If the Commission's efforts are to succeed, the following principles are offered as guidelines in the decision-making process.

- Protecting the security of MVPD networks and upholding the rights of copyright holders to protect against unauthorized use or copying of their works must be given the highest priority. Security must not in any way be compromised or sacrificed for the expediency of achieving commercial availability of navigation devices.

^{5/}See Notice of Written Ex Parte Presentation, dated March 10, 1997, submitted in ET Docket 93-7, Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992--Compatibility Between Cable Systems and Consumer Electronics Equipment ("C3AG Compromise Summary"). Time Warner also actively supports the work of the Security Working Group of the NCTA/EIA Joint Engineering Committee in developing a National Renewable Security System ("NRSS") which is an attempt to forge an industry consensus on portability and eventually interoperability, while protecting signal security in a digital environment.

- Under no circumstances should the Commission allow any device to be made available commercially, absent the consent of the affected MVPD, which can be used by consumers to gain unauthorized access to services delivered by that MVPD. In other words, no device which performs a network security function should be required to be made available commercially.
- The Commission must allow MVPDs to continue to offer integrated navigation/security devices that perform a variety of functions, as long as MVPDs also offer subscribers the option of utilizing commercially available component navigation devices in conjunction with proprietary security devices supplied or authorized by the MVPD.
- The Commission must follow the statutory directive to work with recognized industry organizations in addressing the many difficult and complex technical issues that must be resolved before navigation devices can be made available commercially. Substantial progress has been made in many areas. The marketplace must be allowed to function to achieve the best resolution of these issues and the Commission should intervene only when necessary to ensure continued progress.
- While the marketplace is likely to strive to develop video equipment that is as portable and interoperable as possible in order to satisfy consumer demand, the Commission has no authorization to mandate portability or interoperability of video navigation devices.
- The Commission must clearly distinguish between digital and analog navigation devices. There is a substantial embedded base of largely incompatible analog equipment which cannot be ignored. The cost of replacing this equipment in the short term merely to increase portability and interoperability cannot be justified, especially in light of the eventual transition to a digital environment. Furthermore, as the Commission itself has recognized in the NPRM, analog transmission is inherently less secure than digital transmission. Security concerns alone warrant differential treatment. On a going forward basis, compatibility and portability concerns will be met through the decoder interface standard proposed in connection with the implementation of the equipment compatibility provisions of Section 624A of the Act, 47 U.S.C. § 544a.
- The Commission must ensure that video equipment designated, marketed and sold as "cable ready" provides a sufficiently robust hardware platform to support the downloading and execution of applications, such as program guides, that may be offered to consumers over an MVPD's network. A standardized applications environment and display language, such as HTML, will facilitate portability and interoperability of equipment, while at the same

time ensuring that the equipment is able to support the very services that the equipment is purchased to receive.

There are also some concrete steps which the Commission can take in the short term to facilitate the development of a competitive retail market for navigation devices used to receive multichannel video programming and other services offered by MVPDs without jeopardizing signal security or hampering service and equipment innovation. For example, the Commission could impose the following requirements in the short term:

- Within a reasonable phase-in period, any MVPD which offers equipment combining navigation functions and security functions shall also offer security functions separately in a stand-alone device. Upon development of an acceptable digital interface connector, as has been accomplished with regard to analog devices, unaffiliated suppliers will be free to offer consumers stand-alone navigation devices. Consumers should have the option to either lease or purchase such navigation devices, but MVPDs must be allowed to control availability of security devices.
- MVPDs shall not interfere with a consumer's right to attach any FCC certified navigation device so long as it does not harm the MVPD's network, does not cause signal leakage, and it is not used or useable to facilitate unauthorized reception of service or unauthorized copying of copyrighted material. MVPDs shall take no actions to disable or restrict consumers from using such navigation devices supplied by others in an authorized manner.
- Establish an expedited procedure to revoke FCC authorization of any device shown to cause signal leakage, harm to the network, or which may be used or useful to facilitate unauthorized reception of service.

The following sections discuss these principles in greater detail within the context of the various issues raised by the Commission's NPRM.

II. SIGNAL SECURITY CANNOT BE SACRIFICED TO ACHIEVE COMMERCIAL AVAILABILITY OF NAVIGATION DEVICES.

Although Section 629 provides little specific guidance as to how the Commission is to assure the commercial availability of "navigation devices" to consumers, there are some

specific and concrete statutory limits on the Commission's authority to adopt regulations in this area. Most important of these is the limitation contained in subsection (b) of the statutory provision which unequivocally states that:

The Commission shall not prescribe regulations under subsection (a) which would jeopardize security of multichannel video programming and other services offered over multichannel video programming systems, or impede the legal rights of a provider of such services to prevent theft of service.⁶⁷

Protection of signal security must be the Commission's foremost consideration in promulgating regulations to assure the commercial availability of navigation devices. The most recent available study undertaken by the cable television industry estimates that signal piracy costs approximately \$5.2 billion annually, or approximately 20 percent of the industry's annual revenue.⁷¹ Piracy not only deprives cable operators and copyright owners of their right to be fairly compensated for the product of their investment, but it imposes substantial costs on the honest citizen who is required to bear not only his or her fair share of the costs of programming, but also the share of the freeloading pirate who seeks to obtain product without payment.

While the general desire to foster competition in the manufacture and sale of navigation devices used to receive multichannel video programming services is an important goal which will ultimately benefit consumers, protecting the integrity of MVPD networks from signal theft must be given the highest priority. If MVPDs are hampered in their ability to protect the integrity of their networks, and indeed their very businesses, competition and

⁶⁷47 U.S.C. § 549(b).

⁷¹"NCTA Estimates Loss to Piracy at \$5.2B," Multichannel News (April 14, 1997) at 10. This estimate is based on data collected during 1995 and the first six months of 1996.

consumers will be harmed in the long run. Indeed, the magnitude of the potential harm is significantly increased, not decreased (as many blithely assume), as video distribution technologies transition from an analog to a digital environment. While it is true that digital encryption schemes should be generally more difficult to defeat than their analog counterparts, the repercussions of a breach in digital security are far more extreme. In a digital environment, the ubiquity of low cost computing power and the computer's ability, given the proper programming, to emulate most any piece of electronic hardware, gives the user the ability to create an unlimited number of unauthorized perfect copies from a single authorized source. The Commission must take special care to ensure that the interests of copyright holders are fully protected and not sacrificed merely for the expediency of achieving commercial availability of video navigation devices.

Accordingly, the Commission must take care to ensure that the navigation devices which are to be made commercially available are not defined to include equipment which performs security functions. For example, the NPRM loosely uses the term "converter" in a way which might be read include all equipment used to receive multichannel video programming services, including integrated converter/descramblers descramblers.^{8/} A true

^{8/}NPRM at ¶ 14. The Commission indicates its belief that the policies underlying Section 624A of the Communications Act (the "Eshoo Amendment"), requiring the Commission to adopt the most general of guidelines to foster equipment compatibility, leave the details of implementation to the marketplace, and separate security from the functions and features to be available in the competitive marketplace, are limited to that statutory provision and do not necessarily apply to regulations adopted pursuant to Section 629. NPRM at ¶¶ 35-36. This represents an overly restrictive view of the statute. Contrary to the suggestion in the NPRM, the statutory policies underlying Sections 629 and 624A are in harmony. There is no support in either the statute or legislative history that would indicate that Congress intended to require descramblers, decoders, or other security equipment to be sold at the retail level. Indeed, such a requirement would directly contravene the policies set forth in Sec. 629(b).

converters is essentially a tuner, but certainly not a descrambler. The statute requires regulations assuring the commercial availability of *converters* and specifically prohibits the FCC from adopting regulations which would compromise signal security or diminish the rights of copyright holders, such as regulations requiring retail availability of descrambling equipment. Devices providing security functions, whether digital or analog, must be excluded from the commercial availability requirement.^{9/}

There are three crucial steps requiring interindustry consensus which must be completed before the goals of Section 629 can be accomplished. First, harmonization of the commercial availability desires embodied in Section 629(a) with the security concerns underlying Section 629(b) will require ultimately that security functions be separated from non-security functions in commercially available video navigation devices. Second, the Commission must require that any digital video navigation device that is commercially available be equipped with the proper security to prevent digital signals from being delivered in the clear at the output of the device or utilize an appropriate interface that will prevent unauthorized copying and piracy. Third, the Commission must not establish any "right to attach" devices to an MVPD's network which can be used to facilitate unauthorized reception of service and must make its equipment authorization procedures more stringent to avoid

^{8/}(...continued)

Furthermore, the colloquy between Senators Faircloth and Burns during the Senate debate on the Conference Report provisions dealing with Section 629, cited in Section V of these comments, clearly indicates that the very same policy of minimal government intervention embodied in the 1996 Eshoo Amendment to Section 624A of the Act also underlies Section 629.

^{9/}See H.R. Rep. No. 204, 104th Cong., 1st Sess. 112 (1995) ("The Committee does not endorse any particular method for providing security and does not authorize the Commission to adopt regulations which would jeopardize the security of a telecommunications system.").

inadvertently authorizing devices manufactured to facilitate signal piracy. Each of these points will be discussed in turn.

A. Separation of Security and Non-Security Functions.

The only way to balance the desire to make navigation devices commercially available while still protecting the security of MVPD networks is to separate security functions from non-security functions contained any such devices. The Commission has already endorsed this approach in its ongoing proceeding to implement the equipment compatibility provisions added to Section 624A of the Communications Act by the 1992 Cable Act. The regulations to be adopted pursuant to the equipment compatibility provisions of Section 624A, based on the work of the C3AG, are expected to provide adequate incentives to foster the development of a competitive market for non-security related devices in the analog environment. The decoder interface connector specification to be finalized in that proceeding represents precisely the type of interindustry cooperation that is required under Section 629. It also addresses the need to separate security functions from non-security functions in the analog environment on a going forward basis.

The analog decoder interface compromise achieved by the C3AG provides a good starting point to develop an analogous approach for the digital environment. Indeed, Time Warner has been actively involved in the development of a National Renewable Security System ("NRSS") that should facilitate the widespread commercial availability of navigation devices by establishing a common interface for a renewable and removable security module to be used with digital navigation devices. Presently there are two NRSS options under development. NRSS-A consists of a conditional access interface controlled via a removable chip (commonly referred to as a "smart card"). The security processor continues to reside in

the navigation equipment. NRSS-B consists of a PCMIA-type interface which would allow both the smart card *and* security circuitry to be removed *and* replaced if needed.

Time Warner believes that the approach embodied by the NRSS-B, whereby *all* security functions can be segregated from commercially available navigation equipment, shows far more promise than alternative approaches to protect security in a digital environment. Experience in Europe, Latin America and elsewhere with smart card type conditional access systems has repeatedly demonstrated that the ability to change the conditional access function (*i.e.*, smart card) without the ability to change the underlying security circuitry will not allow for adequate recovery in the event the underlying encryption scheme is compromised or defeated.

Although digital transmission is inherently more secure than analog, there is no security system which cannot be breached. It is not a matter of whether digital encryption schemes will be defeated, but rather a question of how long it will take to defeat a particular security scheme and whether security can be recovered at an acceptable cost. Already the internet is rife with articles and other information providing road maps and "how to" manuals on such subjects as reverse engineering, decryption, obtaining "cloned" smart cards and other methods to defeat current digital security methods.^{10/} In other countries, the methods used by hackers to pirate service have been fairly sophisticated. The proliferation of unauthorized "smart" cards come equipped with the means to connect these cards to pirate sources via modem to update them as existing legitimate cards are replaced. The only solution is to require a modular security system that will allow the entire security module,

^{10/}Examples of the type of information available on the Internet designed to aid "hackers" are included as Exhibit A to these comments.

not just the conditional access (smart card) function, to be replaced by the MVPD in the event of a security breach.

B. Protection Against Unauthorized Copying.

The transition to a digital environment will require the development of interface protocols which allow decrypted digital signals to flow directly to the final display circuit of consumer video equipment, but *not* to any circuit where such decrypted signals can be stored, forwarded, copied, or exported from the relevant device. The Commission must recognize that the availability of powerful yet inexpensive computers which can be programmed to emulate any kind of consumer electronics, coupled with the fact that it is possible to make an unlimited number of unauthorized perfect copies from a single authorized digital source, dramatically increases the consequences of piracy and copyright infringement by several orders of magnitude.^{11/} Accordingly, the FCC must require that any digital video navigation device that is commercially available either be equipped with the proper security to prevent digital signals from being delivered in the clear at the output of the device, or utilize an appropriate interface that will prevent unauthorized copying and piracy.

Time Warner has supported the efforts of the multi-industry Copyright Protection Technical Working Group ("CPTWG") to develop and implement an effective system to prevent unauthorized copying of motion pictures and other filmed entertainment on prerecorded digital video disc ("DVD") media. The work of the CPTWG has resulted in an interindustry agreement to equip DVD players with circuitry which prevents the unauthorized

^{11/}While the problems relating to unauthorized copying of analog videos should not be minimized, each generation of copy from an analog source is somewhat degraded from the previous generation, which to some extent has deterred widespread unauthorized copying of analog videos. With a digital source, however, unlimited perfect copies are possible.

copy or playback of material that has been encoded with copy protect technology and allows equipment manufacturers to license the encryption system for any product where DVD playback is desired. While additional work will be necessary to expand this scheme to services offered over MVPD networks, Time Warner believes that this work represents a promising starting point for achieving an interindustry agreement to create an acceptable interface to ensure that copy protection schemes may not be bypassed by delivering unencrypted digital signals in the clear at the output of any device prior to the final display circuitry of the television receiver or other terminal equipment.

C. No "Right to Attach" Should Apply to Devices Used or Useful to Facilitate Unauthorized Reception.

The Commission tentatively proposes to incorporate the basic Carterfone principle^{12/} into its rules regarding the commercial availability of navigation devices, *i.e.*, attachment must be permitted so long as the devices do not adversely affect the network and are privately beneficial without being publicly detrimental.^{13/} To the extent that the Commission creates a Carterfone-based "right to attach" devices to an MVPD's network, however, it should limit this right to: 1) devices which do not interfere with services and functionalities, including navigational software, branding information (*e.g.*, logos, icons, promotional materials, company identifiers, etc.), and pay per view ordering functions, offered by the MVPD; 2) devices which do not harm the network, *e.g.*, through introduction of spurious upstream data or by causing signal leakage; and 3) devices which are not used or

^{12/}See Use of the Carterfone Device in Message Toll Telephone Service, 13 FCC 2d 420, 13 RR 2d 597 (1968), *recon. denied*, 14 FCC 2d 571, 14 RR 2d 185 (1968).

^{13/}NPRM at ¶ 56.

useful to facilitate unauthorized reception of service. Without such limitations, signal piracy cases will become much more difficult to prosecute, in violation of the Section 629(b) mandate that the Commission not prescribe regulations which would jeopardize the security of services offered over MVPD systems or impede the legal rights of MVPDs to prevent theft of service.^{14/} In other words, consumers should *not* have a right, under a Carterfone-type principle, to attach any device to an MVPD's network which has not been authorized by the FCC and which is capable of facilitating theft of service or unauthorized copying.^{15/} A corollary of this principle is that MVPDs would not be allowed to take any action to disable or restrict consumers from obtaining authorized services using authorized navigation devices supplied by unaffiliated parties in an authorized manner, and that the FCC establish procedures to revoke the authorization for any devices which do not satisfy the foregoing criteria.

Given that FCC approval of devices is part of this proposal and based on its experience in attempting to prosecute manufacturers and distributors of pirate descramblers, Time Warner believes that the Commission should make its equipment authorization process

^{14/}Time Warner has been involved in a number of piracy cases where the defendants have attempted to argue that their sale of modified descramblers was not illegal because the equipment had originally received FCC authorization pursuant to procedures set forth in Part 2 of the Commission's rules. The establishment of a legal "right to attach" without an appropriate authorization requirement will allow unscrupulous pirates to raise another argument which will make prosecution more difficult.

^{15/}In addition, the Commission must understand a fundamental difference in applying the *Carterfone* principle in the MVPD context. Unlike in the telephone context, where the attachment of faulty CPE only harms a single line, attachment of defective MVPD CPE, particularly when used to transmit information upstream, could potentially harm the entire network, and disrupt service to all subscribers. Similarly, a faulty device can result in signal leakage and potential interference with vital safety of life radio services.

more stringent as it relates to obtaining approval for cable system terminal devices ("CSTDs"). The simplicity and relaxed showing required to authorize a CSTD under the present notification procedures has allowed companies (some of whom are believed to be affiliated with individuals adjudicated to have been engaged in signal piracy) to obtain FCC authorization for devices which have not, to Time Warner's knowledge, been purchased or authorized for use by a single legitimate MVPD, but which are nonetheless capable of defeating a number of scrambling schemes commonly utilized to secure MVPD services. These companies often trumpet this FCC authorization as if it should provide cover for any use of the devices, including unauthorized receipt of service.

Time Warner is aware that the Commission has tentatively proposed to upgrade the process of obtaining equipment authorization for CSTDs from notification to certification "to ensure against the marketing of such devices for theft of service."^{16/} This is an essential step to retard the manufacture and distribution of equipment used to pirate MVPD services. However, additional procedures, applicable specifically to CSTDs, should be implemented as well. These include:

- requiring a detailed description of the features contained in the equipment for which approval is sought which are designed to prevent unauthorized access to programming, and to prevent unlawful modification of the equipment;
- requiring applicants to detail steps taken to ensure distribution of the equipment by legitimate cable equipment distributors, *e.g.*, so equipment cannot be altered and then distributed on the black market;

^{16/} See Notice of Proposed Rulemaking in ET Docket 97-94, 62 F.R. 24383 (1997) at ¶ 7.a.

- providing that CSTD authorizations will not become final until 60 days after the public notice of the application grant is published in order to give interested parties the right to seek reconsideration before the equipment is released to the marketplace;
- adopting a standard that prevents unscrupulous companies from manufacturing substandard terminal equipment which allows the conditional access or scrambling/encryption functions to be easily deactivated or bypassed.
- adopting a presumption that entities shown to have any affiliation with any party which has engaged in unlawful theft of service activity within the past ten years may not obtain FCC authorization for any device; and
- establishing an expedited procedure to revoke an authorization where it can be demonstrated that the company or its agent has engaged in illicit theft of service or piracy activities.

Time Warner believes that this proposal can greatly assist both the Commission and private parties to ensure that the Commission's equipment authorization process is not inadvertently used to validate pirate equipment. The requirement to provide greater detail of the security features and marketing practices will provide a means to enable Commission staff to more carefully screen CSTD equipment authorization applications. Public scrutiny of applications after pre-grant, but before equipment can be sold in the stream of commerce, strikes an appropriate balance between the need to protect proprietary information and the need to ensure that the equipment authorization process is not misused by persons seeking to take advantage of minimal public disclosure to obtain approval for equipment that is manufactured for the pirate market. A 60 day delay between approval and marketing will not place a severe burden on legitimate equipment manufacturers or unduly delay their ability to bring new products to market in an expeditious fashion. However, the opportunity for public scrutiny of these applications following pre-grant can be expected to minimize the incidence of equipment authorizations being granted inadvertently for pirate equipment.

III. EQUIPMENT AND ENTITIES COVERED BY SECTION 629.

A. Equipment Covered.

The NPRM asks which equipment should be considered to be “navigation devices” and thereby covered by any regulations adopted pursuant to Section 629.^{17/} In this regard, the Commission asks how it should distinguish between equipment used by consumers to “access” services offered by an MVPD and equipment used for other purposes.^{18/} The Commission also asks whether it should create specific regulatory distinctions between categories and functionalities of different equipment, such as reception and display devices, access control and security devices, and upstream transmission devices, in order to best effectuate the policies of Section 629.^{19/}

Congress expressly crafted Section 629 with an extremely narrow scope so as to apply only to a strictly limited type of equipment. The statute specifically applies only to “converter boxes, interactive communications equipment, and other equipment used by consumers to *access* multichannel video programming and other services offered over multichannel video programming systems”^{20/} In the NPRM, the Commission correctly recognizes that the equipment covered by this provision is only that used to “access” services offered to consumers by MVPDs, but also suggested that the term “access”

^{17/}NPRM at ¶ 16.

^{18/}Id.

^{19/}Id.

^{20/}47 U.S.C. § 549(a) (emphasis added).