DOCKET FILE COPY ORIGINAL

BEFORE THE

Federal Communications Commission

WASHINGTON, D.C. 20554

RECEIVED
FEB 16 1994
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of:	)	
	)	
Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992	)	ET Docket No. 93-7
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	
	)	

Time Warner Entertainment Company, L.P. ("Time Warner"), by its attorneys, hereby replies to certain of the issues raised by the comments submitted in response to the Commission's Notice of Proposed Rulemaking in ET Docket No. 93-7 ("NPRM").[1] Specifically, certain of the comments filed in this proceeding go far beyond the issues raised in the Commission's NPRM by proposing that the Commission limit the provision of interface hardware by cable companies and establish a requirement that cable operators implement a software-based conditional access renewable security method such as the yet to be developed "smart card" technology.[2] These commenters argue that it is necessary to have processing, descrambling and decompression functions built directly into consumer electronics hardware, rather than be provided separately by the cable operator, in order to prevent cable service providers from having a monopoly on the hardware used to receive their services and unfairly

[1] Notice of Proposed Rulemaking in ET Docket No. 93-7, FCC 93-495, _____ FCC Rcd. _____ (released December 1, 1993).

[2] See, e.g., Comments of Circuit City Stores, Inc. ("Circuit City") (arguing that any hardware provided by cable operators must be strictly limited to descrambling circuits); Comments of Mitsubishi Electronics America, Inc. ("Mitsubishi") (arguing that all security hardware must be standardized and that cable operators control access to secured programming through the use of proprietary software); Comments of The Titan Corporation ("Titan") (arguing that only access control functions of signal security hardware should remain proprietary while decoding functions be standardized).

No. of Copies rec'd 0+9
List ABCDE

extract monopoly profits from the consumer.[3] Furthermore, it is argued that the standardization of digital compression, transport and processing is required in order to prevent the national information infrastructure from developing into a "Tower of Babel,"[4] thereby recreating the compatibility problems which developed in the analog world and which Congress sought to address in enacting Section 624A of the Cable Television Consumer Protection and Competition Act of 1992 ("1992 Cable Act").

A. Retail Availability Of Descrambling Equipment Is Not Required To Realize The Benefits Of Competition

At the outset, Time Warner wishes to make clear that it has no objection to the long term general goal of creating a competitive marketplace for interface equipment that will be developed to provide new services over the evolving national information superhighway. Time Warner disagrees, however, that the standardization and retail availability of descrambling and other proprietary security hardware is necessary to allow the public to realize the benefits of competition. Given the fact that customer premises equipment provided by cable operators will be regulated on the basis of actual cost pursuant to the Commission's rate regulations, the notion that cable operators will be able to extract "monopoly profits" from the provision of such equipment unless that equipment is also available competitively at the retail level is a red herring. Furthermore, the Commission should take note of the fact that cable operators, including Time Warner, are not significantly involved in the manufacture of cable television customer premises equipment. Rather, most such equipment is manufactured by well known consumer electronics equipment suppliers such as Pioneer, Panasonic, Magnavox, and Zenith. Cable operators are in the business of providing services, not hardware, and already have an incentive to keep equipment costs to the consumer as low as possible so that consumers will use

---

[3]Circuit City Comments at pp. 3, 10; Titan Comments at p. 5.

[4]Mitsubishi Comments at p. 8.

their discretionary income to purchase additional services. Thus, increased competition at the manufacturing level, whether through licensing or other arrangements, would result in cost savings to both cable operators and consumers alike.

B. Standardization And Retail Availability Of Signal Security Hardware Poses Significant Risks And Costs

Some consumer electronics manufacturers argue that by allowing signal security, decoding, and decompression circuits to be built into consumer electronics products which are competitively available at the retail level, equipment redundancies can be avoided and cost savings to the consumers can be achieved. As to the redundancy aspect, these arguments must be viewed skeptically when made by an industry that has failed to avoid redundancy in its own field by establishing such incompatible video formats as VHS, Beta, 8mm and laser discs, and such incompatible audio formats as records, audiotape, 8 track, digital audiotape and compact discs. Furthermore, this argument also ignores the fact that one of the purposes of the decoder interface standard proposed by the Commission is to eliminate the need for redundant equipment and to do so without compromising signal security.

Advocates of retail availability of security hardware also downplay or entirely overlook the substantial risks and costs inherent in such an approach. For example, retail availability of security hardware would require standardization of the scrambling schemes now currently utilized throughout the United States. Given the fact that there are approximately a dozen different scrambling approaches currently used by cable operators to secure their signals, the standardization of scrambling and descrambling functions would make obsolete a substantial portion of the customer premises and headend equipment that is currently in place. The replacement of this equipment would impose tremendous cost burdens upon the cable industry, and ultimately cable subscribers, which could delay implementation of new and promising

technologies that also require significant capital expenditures, such as the deployment of fiber and digital video compression.

More importantly, however, the most severe problem with a single scrambling standard is a lack of alternatives if it is defeated. The experience in the United States, the nation which by far enjoys the highest penetration of cable and subscription video, is that every signal protection scheme, over time, suffers an increasing degree of compromise as pirates develop and market illegal devices. According to the Office of Cable Signal Theft ("OCST") of the National Cable Television Association, in 1991 alone, over 1,300 theft of service cases were prosecuted nationwide on federal, state and local levels. Seventy-five percent of the more than 250,000 devices seized by law enforcement agencies in 1991 were capable of circumventing addressable technology and allowing illegal reception of pay-per-view services. OCST has estimated that each illegal decoder sold to a consumer cost the cable industry approximately $3,108.00 over the decoder's useful life. Contrary to the assertions of Titan Corporation, adoption of a single uniform scrambling standard would exacerbate, not mitigate, the theft of service problem by creating a national market for pirate decoders.[5] Indeed, the lucrative nature of signal piracy is illustrated by the fact that the president of the National Consumer Cable Association, a trade association representing the manufacturers of "competitive" signal security hardware, was recently charged with two felonies related to the distribution of unauthorized cable descramblers. In that single case, it was reported that 70,000 unauthorized devices were seized.[6] The establishment of a national scrambling standard will accomplish little more than providing further incentives to manufacture illegal descramblers by creating a national market for such devices.

---

[5]Titan's assertion that loss of $4.7 billion by the cable industry to signal theft in 1991 despite the use of a dozen different scrambling systems somehow demonstrates that a single national security standard would be less vulnerable to compromise is a non sequitur. See Titan Comments at p. 5, n. 9.

[6]"Descrambler Foe Charged in L.A.", MultiChannel News, December 6, 1993 at p. 81.

The problem of maintaining signal security is greatly exacerbated in cases where cable operators lose control of security hardware, such as in a situation where descrambling equipment may be legally purchased by subscribers either as part of their TVs or in VCRs, or as stand-alone units. Subscribers are less reluctant to tamper with their own hardware than with the equipment which belongs to the cable company. Prosecution for tampering becomes impossible as a practical matter if the cable operator does not own the descrambler. Moreover, if descramblers become available commercially, it will be extremely difficult to determine whether a particular descrambler was legally manufactured and subsequently tampered with, or whether it was originally manufactured to defeat an existing security system. Thus, it would become much more difficult to successfully prosecute the manufacturers of illegal descramblers, who up to now, have been a primary target of theft of service investigation and enforcement.

Allowing subscribers to purchase their own descramblers from a variety of commercially available sources would also take away one of the significant weapons used by cable operators and equipment manufacturers to combat signal theft. In cases where security has been compromised, it is often possible for the manufacturer and cable operator to make a few changes in the security system that will deauthorize the illegal descramblers while allowing authorized subscribers to continue to receive the programming they purchased without the necessity of changing their equipment. Such an approach would be difficult or impossible in a situation where descramblers in the field came from a variety of manufacturers. Because of the different manufacturing techniques and processees, it may not be possible to guarantee that the changes implemented to recover security would deauthorize only illegal decoders. This would create anger and frustration in cases where legitimate subscribers would no longer be able to use their purchased descrambling equipment on the cable system.

The ultimate defense against compromise of a security signal is to replace the compromised system with a better one which builds on the lessons learned from the previous

defeat. Thus, when the degree of compromise becomes intolerable from a business standpoint, the cable operator replaces signal protection hardware. The subscriber's investment in their TVs and VCRs is not affected. If a single scrambling or encryption method were required and then later compromised, there would be no way to recover security without rendering the subscriber's equipment unusable. This would result in subscriber anger at having at least part of his or her investment rendered useless. Ironically, the focus of this anger is likely to be the cable operator and not the manufacturer who sold the TV or VCR with the now useless equipment.

The highly touted "renewable" security methods, which would allow security to be updated when compromised without requiring new equipment to be placed in the home, are a partial solution at best, and may not be a solution at all.

First, an important fact not acknowledged by the proponents of a renewable software-based conditional access security scheme is that even after digital television becomes a reality, analog television will continue to be provided over broadband networks, such as cable systems, due to cost and other considerations. Thus, differing analog and digital security systems may be required to function side-by-side in the same network environment, whether or not a so-called "smart card" is used with either of the systems.

Second, with respect to the delivery of analog signals, the use of a smart card, which contains the addressability information allowing authorization of a particular descrambler unit to receive a particular service, is ineffective to prevent signal theft in cases where the video scrambling scheme itself has been defeated. In those instances, the addressability function is not needed to authorize descrambling and is effectively bypassed. Accordingly, just being able to replace the addressability control by sending out a new smart card does not recover security. The entire signal protection method, including the descrambler, must be replaceable in order to maintain security. The smart card approach works best in those limited instances where security has been compromised because the addressability system has been fooled into authorizing

descramblers to receive programming which had not been ordered. In these cases, replacement of the smart card allows the addressability system to be changed without the need to replace the entire descrambler unit.

Third, even with respect with digitally delivered signals, the smart card approach, although very promising, should be approached cautiously.[7] No signal protection system is "unbeatable." Those who design signal protection methods have limited time, limited personnel and limited budgets. They make their designs at a point in the evolution of technology based on assumptions of limited access to that technology. Those who would compromise a security system have unlimited time and the ability to do it at their leisure as a hobby. While digital technology does provide more tools to the designer of security systems, it also provides more tools to the attacker. The computer "hacker" has available incredibly complex and capable computing power at very low prices. Networking techniques have made it possible for groups of hackers to rapidly share the results and their computing power. New and even more powerful personal computers and networking systems are promised in the near future. The mere possibility of defeat and the absence of a recovery alternative should be a sufficient reason for the Commission to refrain from mandating a particular signal security approach at the present time, whether it be for analog or digital video signals.

C. The Commission Should Not Stifle The Development Of Newly Emerging Technologies And Services By Prematurely Establishing Digital Transport And Processing Standards

Apart from the signal security issue, the Commission should decline the invitation to prematurely establish standards for the delivery of digital programming to the home just so that

---

[7]Because of their small size and low cost, smart cards might well present a particularly attractive and lucrative target for pirates. A subscriber purchasing an inexpensive pirate smart card would probably be far more likely to purchase subsequent "updated" pirate smart cards as the conditional access authorizations are altered than they would be to invest in an expensive replacement hardware unit.

decompression and processing equipment can be built directly into the next generation of television sets and VCRs. It is Time Warner's belief that where various components of a digital delivery system have been standardized, there is no reason that they should not be offered competitively, much the same way as converters/tuners are now readily available in the marketplace. However, in light of the dynamic nature and rapid pace of technological change, and the embryonic stage of digital television, the Commission must be careful not to prematurely set standards that will stifle the development of new services. While some commenters advocate linking digital television standards to the process underway to develop High Definition Television,[8] the Commission must not lose sight of the fact that a standard for digital compression is just one element of the total system. The other components include: 1) a modulation technique; 2) an addressability and conditional access method; 3) demultiplexing means to select an individual channel from the multiplexed digital carrier; 4) Time Domain Equalizer training signals; and 5) error detection and correction schemes. At present, a lack of operating experience prevents a clear understanding of the impact of these factors on compatibility. Indeed, the concept of the information superhighway is not just to transport digital television but a whole new array of communications services that may include audio, voice and data services that are not even intended for connection to a television set. The Commission must not allow the desire of hardware manufacturers to sell more televisions sets to limit the development of these new services under the banner of standardization.

The Commission's proposal to adopt a decoder interface standard that will work for both analog and digital transmission is a reasonable first step in establishing standards for the delivery of video programming in a digital world. Furthermore, Time Warner believes that, in the short to mid-term, a compression standard will be developed that will allow this function to be

---

[8]Mitsubishi Comments at p. 7.

available competitively, both by integrating decompression equipment into newly manufactured televisions and video cassette recorders and by the manufacture of component stand-alone decompression devices which can be connected to existing and newly manufactured consumer electronics equipment.

Digital transport and processing standards are quite another matter. Cable operators and other multichannel video distributors must remain free to experiment and employ different digital transport and processing methods to maximize network cost efficiencies and provide an incentive to invest capital to develop a national communications infrastructure. With many new wire based and wireless technologies just now beginning to converge and compete in the marketplace, the use of a particular digital transport or processing technique must be dictated by bandwidth needs, network architecture and design, service demands and traffic management needs. The differing service and technical characteristics of direct-to-home satellite broadcasts, terrestrial broadcasting (including high definition television), cable television systems, and wireless technologies such as MMDS and LMDS, virtually assure that the most efficient signal processing and digital transport techniques used for one technology will not transfer equally well to competing technologies. The Commission should not stifle competition between these emerging and established technologies by imposing a uniform transport and processing standard which has been developed for any single technology.

Finally, in seeking to encourage the development of a national information infrastructure, the FCC must not lose sight of the fact that the underlying purpose of hardware deployment is not for its own sake, but rather as a means of facilitating the exchange of information, entertainment and transactional services. Some of these services exist now, while others have not yet been developed. As new services emerge and as service providers experiment with offering old services in new ways, network operators must be free to develop hardware that will allow the retrieval, manipulation and use of the information to be accomplished in the most user-

friendly fashion. In the long term, it may even be possible to establish standards for certain transport and processing functions.[9] The way to accomplish this is not by prematurely setting standards that will rapidly become outmoded and that will ultimately stifle the development of new services. Rather, the marketplace should be allowed to evolve with maximum flexibility and incentives for experimentation. Such an approach will ensure that once standards are ultimately set, they will be based on marketplace proven technologies and efficient economical network designs which have succeeded in meeting the consumer demand for service.

Respectfully submitted,

TIME WARNER ENTERTAINMENT
COMPANY, L.P.

By: Howard S. Shapiro

Arthur H. Harding
Howard S. Shapiro

Fleischman and Walsh
1400 Sixteenth Street, NW
Sixth Floor
Washington, D.C. 20036
(202) 939-7900

Dated: February 16, 1994

Its Attorneys

13460

---

[9]This is not to say that cable operators and other network providers should not strive to deliver their services in a manner compatible with existing and newly manufactured consumer electronics equipment. For example, all providers of analog video services should be required to comply with the compatibility standards established in this proceeding or else the benefit of these standards is significantly diminished. Although one commenter has suggested that any standards established by the Commission do not apply to video dialtone services, since such service and facility providers are not considered "cable operators" (Bell South Comments at pp. 1-3), Section 624A(d) of the 1992 Cable Act makes clear that the Commission's authority to promulgate regulations in this area is limited not only to cable systems, but also covers "similar technology."