Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Video Device Competition	)	MB Docket No. 10-91
	)	
Implementation of Section 304 of the Telecommunications Act of 1996	)	
	)	
Commercial Availability of Navigation Devices	)	CS Docket No. 97-80
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	PP Docket No. 00-67

NOTICE OF INQUIRY
Comment from SypherMedia International, Inc.

SypherMedia International (SMI), a Pay TV security technology company, is pleased to submit comments on the "Notice of Inquiry (Video Device Competition; Implementation of Section 304 of the Telecommunications Act of 1996: (Document ID FCC-2010-0143-0001))".

The concept of a "gateway device" is very intriguing if implemented with adequate security protections, but the approach also creates significant security risks which must be addressed to prevent catastrophic security consequences. We are very fortunate that new security technologies are available today to address the short comings that hurt the Cable Card initiative and that these new security technologies will help to resolve the barriers to bring multiple MVPD devices to the market.

Listed below are responses to selected questions and statements taken from the Notice of Inquiry Document ID FCC-2010-0143-0001.

I. Introduction

1. In particular, we wish to explore the potential for allowing any electronics manufacturer to offer smart video devices at retail that can be used with the services of any MVPD and without the need to coordinate or negotiate with MVPDs.[1] We believe that this could foster a competitive retail market

[1] The term "smart video device" refers to a product that is capable of navigating the universe of video content available to a viewer. Traditionally, these devices have been cable or satellite set-top boxes, but have expanded to include video game systems, digital video recorders, and home theater personal computers, and which, with the AllVid adapter could additionally provide access to over-the-top services like internet video.

in smart video devices to spur investment and innovation, increase consumer choice, allow unfettered innovation in MVPD delivery platforms, and encourage wider broadband use and adoption.

SMI supports aspects of the Initiative:
SMI supports aspects of this initiative and agree that opening a competitive retail market for devices that have access to additional and/or optional MVPD services will benefit the consumer. An example of how that is happening today would be the multiple video services that Blu-ray player device manufactures are offing. Many internet enabled Blu-ray players also offer Netflix and Amazon movie downloads via a wired or wireless connection. Although this is a very limited offering, it points to the Smart Video Device and AllVid concepts discussed herein and validate the notion of a single device purchased at retail can support more than a single source of content.

2. More specifically, we introduce the concept of an adapter that could act either as a small "set-back" device for connection to a single smart video device or as a gateway allowing all consumer electronics devices in the home to access multichannel video programming services.

Backward compatibility is a critical challenge to quick adoption:
Having an adapter or set-back device addresses the issues of backward compatibility and may open an existing device to new services if those services utilized a standardized security approach. Without a standardized approach the set-back device would ultimately become too complicated and therefore too costly. The primary technical challenge is to ensure that the input or output from the "set back" devices will not facilitate piracy of content.

3. The Commission envisions that the proposal adopted in this proceeding would be a successor technology to CableCard.

New technology is available to replace CableCard security functionality at a fraction of the cost and complexity:
The successor to CableCard needs to address all of the pertinent issues that inhibited wide scale adoption. Cost, size, and use flexibility need to be addressed and new solutions brought forward. A proposal to solve these issues is addressed in the General Comments section below.

7. The Commission adopted its first Report and Order to implement Section 629 in 1998.[2] The order required MVPDs to make available a conditional access element[3] separate from the basic navigation device, in order to permit unaffiliated manufacturers and retailers to manufacture and market navigation devices while allowing MVPDs to retain control over their system security.[4]

A common security gateway that does not require unaffiliated manufactures to certify new products is the key to the initiative success:
This is a key provision and must be solved in an innovative and cost sensitive approach to enable this initiative to succeed. The solution lies in having a robust universal security device, with a hardware root of trust that can co-exist with additional and/or proprietary security system(s) to manage the conditional access and/or digital rights management of specific content/operators. This technology is the gateway to true "downloadable security". This technology exists today and is discussed in detail in the General Comments section below.

15. First, with few exceptions retail navigation devices are unable to provide functionality beyond that available in devices that a subscriber can lease from their providers and often are unable to access many of the MVPD services that leased set-top devices are able to access. Second, as a general matter a retail navigation device purchased for use with one MVPD's services cannot be used with the services of a competing MVPD.

A Universal Security Gateway allows for multiple MVPD access:
Limited multiservice devices are available as discussed in the response to section 1 above. This can be greatly expanded if a universal security gateway is adapted to provide common access to the devices. In the example given, the Blu-ray manufacturer must integrate a separate solution for both Netflix and Amazon. While player manufacturers can integrate a few major services, player memory, hardware constraints, engineering integration resources, and other practical considerations limit the number of services that can gain widespread adoption via this ad hoc process. A universal security gateway would allow Consumer Electronics device manufactures to open their devices to any content provider via an open distribution interface such as off-air ATSC and the Internet greatly expanding the access to content. If implemented without adequate security, however, the universal gateway would also provide unfettered access to pirates. As a result, the success of the open platform

---

[2] *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices*, 13 FCC Rcd 14775 (1998) ("*First Report and Order*").

[3] The term "conditional access element" refers to a piece of equipment that handles the security functions that allow a navigation device to access subscription video services (*e.g.*, decryption of scrambled content).

[4] *Id*. at 14808, ¶ 80; 47 C.F.R. § 76.1204(a)(1).

envisioned in this paper depends entirely on whether sufficient security technologies and associated robustness requirements are required.

28. *Encryption and Authentication*. Both the MPAA and CableLabs have approved digital transmission content protection over Internet protocol ("DTCP-IP") technology as an acceptable method of content encryption to prevent content theft, and it is the content protection scheme used in the Digital Living Network Alliance ("DLNA") standard.

DTCP-IP is not the security solution for this Initiative:
SMI does not agree that DTCP-IP is the correct standard to use. It could possibility lead to irreparable harm to content owners and subsequently lead to restrictions of certain high value content from ever reaching consumers via the methods envisioned. The gold standard for Pay TV security is hardware based security with built in protections from reverse engineering, differential power analysis attacks, and unique device keys. DTCP-IP is a link protection mechanism, like HDCP, it is worthy technology for the carriage of "in-the-clear" compressed content to a trusted "secure" decoding and display device.

A non "secure" decoding device would allow compressed content to be stolen, from memory buses or device interfaces (using malware). Compressed content should ideally be descrambled, decompressed and decoded in a "secure" environment ideally all within a single SoC. As a link protection mechanism, DTCP-IP does not protect content that is intended to be persistent on the recipient device.

Supporting a range of content delivery models including pushed ahead VoD, down-loaded purchased content, and downloaded rental content (e.g. play once). Content protection mechanisms, like the CryptoFirewall discussed in the final section "General Comments", can support these models and are agnostic to the delivery format transport (MP2, MP4) or package types (PIFF) and compressed content types (MP2, MP4, SVC, Flash etc). Further the content protection mechanism must provide protection for content delivery and persistent content stored within a platform.

The content protection mechanism must also be co-located with the content descrambling and decompression processes in a "secure" decoding SoC on a single chip. Integration of decoding and security reduces costs by avoiding the need for a separate security chip, and also improves security by eliminating external buses and interfaces that can be subject to attack. A "secure" decoding device provides a mechanism to prevent in-the-clear compressed content from being stolen, through the use of secure interface technologies like DTCP-IP, HDCP, etc. and the use of hardware based robustness techniques such as the CryptoFirewall to protect key material, protect content on exposed buses (including memory, debug), and prevent the execution of unauthorized software (or malware).

General Comments:
An example of a specific security technology that can help address many of the security challenges with the AllVid proposal, we recommend that the FCC consider the CryptoFirewall IP Blocks from the U.S. semiconductor security firm Cryptography Research Inc. This tamper-resistant technology can be added to any chip, and is already used in existing pay television services. Four of the leading Consumer Electronics (CE) chip manufactures will be offering this security technology in their chips. These chip manufactures represent 90% + of the United States cable and satellite Set Top Box market today. This security ASIC can and will be integrated into additional chip manufactures products going forward furthering an even larger chip market from which to choose from. This security ASIC provides significantly more security as compared to CableCard and at a significantly lower cost. Since the CryptoFirewall is integrated directly into the CE device transport chip, or System on a Chip (SoC), there is no additional footprint required for the device manufacture to incorporate. Cost is typically a onetime $1.00 or less.

SMI has integrated an assortment of different security technologies and prefers the universal nature of the CryptoFirewall platform. For example, a cable customer could move to a different cable operator and activate the same retail-purchased set top box by simply reading the STB ID to the new operator (or, if the network is two-way, transmitting it automatically). The new operator would use their backend Conditional Access or Digital Rights management to enable the CryptoFirewall core in the new customer's STB to decrypt the operator's content. Product entitlements would be delivered from the MVPD to the STB, based on the consumer's subscription.

The following is a comparison of the design and operation of CableCard and CryptoFirewall:

a. Cost. CableCard had several cost factors. First the device itself. Early estimates were as high as $70.00 as compared to the CryptoFirewall onetime fee at $1.00 or less.

b. Cost of integration. CableCard required a special chassis with specialized interfaces and power connections. It is relatively large and confines the form factor of the end device. CryptoFirewall is an ASIC integrated into the Transport chip/ SoC. No additional space or power is required. All Televisions and cable/satellite STB's have a SoC. This approach reduces the non-recurring design and manufactures product line setup costs by many thousands of dollars.

c. CE device certification by a third party is not required. The security ASIC is qualified as a function of the SOC to ASIC integration function. Any CE

manufacture can use any CryptoFirewall enabled chip and offer a universal security gateway for any service provider.

d. Gateway to true “downloadable security”. The CryptoFirewall’s hardware root of trust provides the gateway for Conditional Access providers and Operators to innovate software Digital Rights Management and/or Conditional Access software based security which is truly “downloadable”. High value Studio content is secure using both methods in tandem. CryptoFirewall provides protections from a broad range of invasive and noninvasive attacks (e.g., differential power analysis, fault induction, reverse engineering, microprobing, etc.) These built in protections provide the means to protect the software download and work in tandem with any CA or DRM system while providing a more robust solution.

e. Interoperability with existing cable and satellite CA and/or Digital Rights Management systems. CableCard had restrictive issues in this area and added no real advantage in security technology. Systems using CryptoFirewall cores, as previously stated, have an additional layer of hardware security technology that provides built-in protections from a broad range of invasive and noninvasive attacks (e.g., differential power analysis, fault induction, reverse engineering, microprobing, etc.)

f. Universal approach. While CableCard is specific to addressing certain interoperability issues within the cable industry CryptoFirewall was designed to address the new technologies in content delivery. An on-chip security core, such as the CryptoFirewall, in playback devices can sidestep these compatibility complexities by providing a uniform register interface. Having a universal security gateway significantly reduces the cost of the CE device and allows secondary security methods to work together as the operator or service provider desires. The initial contact with the new service would be protected with the CryptoFirewall allowing a secure download of that operators CA or DRM. If the AllVid device is on a two way network this would be transparent to the consumer. If on a one way network the consumer would read the STB device number to the operator for activation.

SMI respectfully submits our comments. We stand ready to support your efforts to enable broader competition for devices that access media services while maintaining robust anti-piracy protections.

Very best regards,

Dennis R. Flaharty
President
SypherMedia International Inc.
5455 Garden Grove Blvd,, Suite 300
Westminster, CA 92683

www.smi.tv