

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

In the Matter of

Downloadable Security Technology Advisory
Committee (DSTAC)

)
)
)

MB Docket No. 15-64

REPLY COMMENTS OF VERIMATRIX, INC.

Verimatrix, Inc. (“Verimatrix”) hereby submits these reply comments to the Media Bureau's Public Notice regarding DSTAC.

I. INTRODUCTION

Verimatrix is the world's leading IPTV security provider and also provides security to the broader content distribution community including satellite, cable and broadband. Overall, we serve more than 800 PayTV operators around the world and protect more than 78 million screens with our Conditional Access (CA) and Digital Rights Management (DRM) systems. In the United States, we are the security provider for more than 100 telephony and cable-based Multi-channel Video Program Distributors (MVPDs) with more than 1 million subscribers. We participated in all public meetings of the DSTAC, participated as invited technical experts on various subcommittees of DSTAC and submitted comments in response to the Media Bureau's Public Notice.

II. MANDATE OF A SINGLE, LINK-PROTECTED INTERFACE WITH UNFETTERED ACCESS TO MVPD CONTENT WOULD PRESENT A SIGNIFICANT SECURITY RISK

Verimatrix notes that the Consumer Video Choice Coalition (“CVCC”) and Public Knowledge submitted comments supporting the initiation of a rulemaking proceeding

based upon the Competitive Navigation and Virtual Head-end proposals.^{1,2} In their respective comments, they assert that the security requirements of MVPDs and their content suppliers would be met by a selected link protection mechanism.^{3,4} Presumably, they desire a mandate requiring broad access to MVPD content across this to-be-defined interface. As we stated in our comments, Verimatrix believes that such a mandate would create a single point of failure for all MVPDs and potentially draw attacks upon the selected link protection mechanism.⁵

In its work, the DSTAC committee decided not to propose the standardization of a single "downloadable security" system. In our earlier comments, Verimatrix agreed with this conclusion since we believe that such an approach would be harmful to competition, innovation and security. Adoption of a mandatory handoff of MVPD content across a link-protected interface as proposed by CVCC and Public Knowledge would have the same effect. It would create a single point of failure, thus harming security. It would also limit the downstream navigation devices to only those usage models supported by the selected link protection system, thus harming innovation. And it would forestall the richer capabilities that could be offered by suppliers of full-capability DRMs, thus harming competition.

¹ CVCC at 11 states, "The DSTAC Report provides the basis for a solution that will fulfill the goals of Section 629 by enabling true retail competition in the navigation devices market. Specifically, the 'Competitive Navigation' solution supported by [CVCC] provides a detailed and practical approach...."

² Public Knowledge in their corrected comments concludes, "The Commission should quickly begin a rulemaking proceeding implementing the virtual head-end proposal."

³ CVCC at 11.

⁴ Public Knowledge at 18.

⁵ Verimatrix at 6.

To illustrate the security problem, we highlight specific errors, oversights and oversimplifications in the comments of Public Knowledge, CVCC, and Hauppauge in the following paragraphs.

Public Knowledge at 18 recommends creating a standard that the MVPDs must support and then asserts that "[it] doesn't require any compromises or changes to the MVPD's security mechanisms, systems, or standards." Public Knowledge also at 18 states that the exemplar link protection system for its proposed standards, DTCP-IP, "has proven more robust to attack" than other listed security systems. There are at least two misleading notions in these assertions. First, even though Public Knowledge does not recommend altering the MVPD-selected security, they recommend terminating its use and passing responsibility for protection over to a government-mandated single point of attack or, more to the point, single point of eventual failure. Second, they attempt to mollify security concerns with anecdotal information that other content protection systems have been brutalized by security attacks in the past more so than the exemplar link protection system. Public Knowledge neglects to point out the truism that pirates are drawn by promise of economic gain. The systems Public Knowledge cited as "less robust" have been subjected to much greater pressure from pirates than the exemplar system. In some cases, lack of breach points not to greater robustness, but instead to lack of sufficient motivation to breach by the pirates. Government mandate of the exemplar system, or any other system as a single point of failure, will draw greater attention from pirates. As we have said previously, Verimatrix systems pass protected content to DTCP-IP in numerous situations. We do not have unique criticisms of that particular security system in the context of its common uses. Our concerns are with the fundamental security problem of having a government-mandated single point of failure.

Software renewability of a downloadable MVPD security system that must, in turn, pass copyrighted content to a government-mandated single point of failure does absolutely nothing to help resolve the security weaknesses of that later stage in the content distribution ecosystem.

CVCC at 11 states, "The security between the cloud and the retail navigation device, through a well-defined, widely-used link protection mechanism such as DTCP-IP allows for secure decryption without requiring that the consumer be tied to a single MVPD and a single user experience when choosing a device." They do not, however, point out that any benefit is at the expense of subjecting the overall U.S. MVPD system to the security weakness of a single point of attack.

Hauppauge at 2 oversimplifies the problem stating "DOCSIS + WG4 services + DTCP-IP = API support for an apps based UI" failing to acknowledge the security risk presented by selecting a single link protection system such as DTCP-IP as a mandated technology standard.

Our security concerns are supported in the comments of Arris, AT&T, and Comcast.^{6,7,8}

⁶ ARRIS at page 7 concurs with our security concerns stating, "[T]he AllVid-type model set forth in the DSTAC Report would require that MVPD supplied in-home server devices use the same link protection security (DTCP-IP), presenting a single point of failure for hackers to exploit." Arris continues, "Section 629 of the Communications Act specifically bars the Commission from promulgating regulations 'which would jeopardize security of multichannel video programming and other services offered over multichannel video programming systems[.]'"

⁷ AT&T at 3-4 concurs with our security concerns stating, "[T]he alternative approach heightens security risks from hackers and unauthorized users by creating a single national point of attack at the interface."

⁸ Comcast at 16 concurs with our concerns about the "increased security risks" of a mandated DTCP-IP link-layer protection for all MVPDs stating that it "would undermine the competitive marketplace for security solutions, create a single, national point of attack vulnerable to hackers, and impose an inflexible security standard that may not be able to respond as quickly as today's various and diverse security systems as such attacks become more sophisticated and complex."

Additionally, Nagra at 3-4 points out two fundamental security-related problems with over-reliance on HTML5 with Encrypted Media Extensions (EME), i.e., vertical lock-in and lack of access to HW protection for 3rd parties. We agree that these are problematic and need to be addressed to facilitate broader utility of the HTML5 with EME. Additionally, EME does not define the mechanisms to download the Content Decryption Module (CDM), i.e., the DRM behind the EME Application Programming Interface (API).

We conclude by reprising this passage from our comments at 7, which seems appropriate in light of the recommendations of Public Knowledge and CVCC.

"Forced standardization suffers the risk of missing the mark and stifling innovation. Forced standardization in security areas suffers the risk of being broken and harming the very markets it intended to facilitate."

Respectfully submitted,

By: Tom Munro

Tom Munro
Chief Executive Officer

Verimatrix, Inc..
6059 Cornerstone Ct W,
San Diego, CA 92121
(858) 677-7800

By: Petr Peterka

Petr Peterka
Chief Technology Officer

Verimatrix, Inc..
6059 Cornerstone Ct W,
San Diego, CA 92121
(858) 677-7800

November 9, 2015