

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

In the Matter of)	
)	
Expanding Consumers' Video Navigation Choices)	MB Docket No. 16-42
)	
Commercial Availability of Navigation Devices)	CS Docket No. 97-80

REPLY COMMENTS OF TECHNICOLOR

Technicolor is a worldwide technology leader in the media and entertainment sector. The company develops technologies for content creators and distributors, Pay TV operators, and over-the-top (OTT) and network service providers for use in mass-market services, devices and platforms. Technicolor's Connected Home business unit offers a wide range of solutions to Pay TV operators and network service providers for the delivery of digital entertainment, data, voice, and smart home services. Through the design and supply of products such as digital cable, satellite, IP and OTT set-top boxes, media gateways and managed wireless tablets, Technicolor offers connected life solutions and enriches consumers' TV experience.

Extensive technical analysis provided in the Comments documents that the NPRM approach for third party distribution of commercial content does not meet acceptable security standards.¹ Technicolor's analysis confirms those deficiencies and has identified other critical

¹ As detailed in the Comments and analysis by NCTA, AT&T, Comcast, Verimatrix, ARRIS, and Cisco, the approach suggested by the NPRM eliminates applications as technological protection measures, fails to provide a trusted application execution environment available on retail devices, artificially constrains the choice of security options, fails to support user authentication, ignores NIST best practices such as network segregation. Such an approach fails to provide a meaningful trust infrastructure within which retail devices can securely access MVPD services. *See, e.g.*, NCTA Comments at 94-96, 97-98, 99; AT&T Comments at 27-28, 45-47; Comcast Comments at 89-90 and Werner Declaration 9-10; Verimatrix Comments at 17-18, 19-20; ARRIS Comments at 13-14; Cisco Comments at 7-8, 9-10, 11, 13.

failures in the security approach proposed by the Notice.

First, the NPRM is proposing a model in which content and data security and the protection of personal information is exposed without clear recourse or penalties for accidental or intentional use or misuse of content or data. As detailed in the DSTAC Report, commercial content and data is protected in today's trust infrastructure through a network of agreements and license obligations that include financial responsibility for compromises, requirements to respond and resolve breaches, warranties, indemnification, rights to audit and other enforcement tools that align financial and operational responsibilities with parties' obligations.² The NPRM relies instead on self-certification but offers no similar enforcement infrastructure to protect commercial content decrypted in the third party device or app, the private information exposed with the "entitlement" information flow, or the television viewing data exposed to the third party. Without clear recourse and penalties for misuse of content or data, any security is merely hypothetical.

Second, the design of the NPRM is to break up and separate the information flows into separate pipes, which increases the risk of compromise. The NPRM currently makes no explicit provision for encrypting the entitlement or service discovery information flows, which has already been identified as an unacceptable risk to privacy.³ But the risk cannot be adequately addressed even by encrypting all information flows. The NPRM begins from a starting point of weakened security by insisting that the only acceptable content protection system must be from the narrow or null set of content protection systems available on RAND terms.⁴ Even if all three separate data streams were encrypted, the NPRM triples the exposure

² Report of Working Group 2 to DSTAC at 24-28 (Final Report of the DSTAC at 51-55).

³ See EPIC Comments at 5-6; Sidney Skjei, A Technical Analysis of the FCC's Navigation Device Proposal (NCTA Comments, Appendix B) (Apr. 22, 2016) at 43-44.

⁴ To our knowledge DRMs are offered as a service, not on RAND terms. Widevine is free, but the NPRM disqualifies

for data breach and nefarious behavior because three encrypted streams provide a hacker with additional data bits that make cracking such encryption easier. Successfully penetrating only one of the streams likely provides access to all streams. Because the NPRM provides no technical or contractual mechanisms for an MVPD to detect intrusion, customer exposure for device compromise and personal information is ripe and inevitable.

Third, the NPRM provides no effective means for validating a device or preventing a device from impersonating legitimate devices. Both the NPRM and the October 20, 2015 filing by Public Knowledge (which the NPRM suggests might be a default solution) lack security certificates that are typically added in manufacturing or embedded in hardware.⁵ The new Technical Appendix offered by the CVCC professes to address a related problem and suggests posting a self-certification on a web page; but any rogue, pirate or hacked device or app could simply pretend to be a compliant device or app by substituting the URL for a known compliant device.⁶ The lack of any meaningful certification program means there is no third party validation of identity or compliance, and without such third party validation there is no security. Rogue devices can impersonate legitimate devices, attack and poison the access network, and import malware into home networks.

Fourth, the NPRM requires that all commercial content of all MVPDs be available through standardized interfaces and a weak security system with no effective recourse or penalties for misuse of content or data. But the same vulnerabilities would not apply to online sources and aggregators, who would remain able to employ all the security and technological

security systems affiliated with MVPDs like Google Fiber. If another system emerges, it will likely rely on the lowest common denominator for content security, information privacy, and searchable premium content.

⁵ See Letter from John Bergmayer, Senior Staff Attorney, Public Knowledge to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Oct. 20, 2015) and accompanying Exhibit (filing *ex parte* letter on behalf of Public Knowledge, Google, Hauppauge, and Amazon and attaching exhibit titled “Implementing the Virtual Headend Proposal”).

⁶ See Technical Appendix to CVCC Comments, MB Docket No. 16-42, CS Docket No. 97-80 (Apr. 22, 2016) at 5.

protection measures available now and in response to future hacks. The NPRM undermines the ability of MVPDs to offer content providers a highly secure distribution platform, and provides an artificial advantage to online video providers who are not encumbered by these mandatory security holes.

Fifth, the NPRM mandates a static security architecture that creates incentives for theft and exploitation of services. Today, MVPDs make use of a diversity of security solutions, can adjust apps in real time, can choose from many CAS and DRM solutions, and can avail themselves of a highly competitive vendor community that continues to improve and enhance security in response to rapidly evolving threats. That diversity and flexibility creates great strength in security. The NPRM model replaces that with a static common point of failure across all MVPDs: three interfaces imposed by technology mandate that cannot be changed without standards-based consensus or regulatory permission; a security system dismantled into a narrow to null set of content protection vendors; and no recourse against third parties accessing the network. This model is incapable of responding nimbly, organically and proactively to any zero-day exploit.

Technicolor has broad international experience in 32 countries. We know of no approach used in any of them that is similar to the proposal in the NPRM. The report submitted by the Technology Policy Institute confirms our experience.⁷ Some participants in this proceeding have suggested “fixes” to the proposed rules through the addition of language prohibiting a third party from interfering with some terms of retransmission consent agreements.⁸ However, the proposal’s overarching deficiencies cannot be fixed with words

⁷ See Scott Wallsten, Technology Policy Institute, An Economic Analysis of the FCC’s Set-Top Box NPRM, MB Docket No. 16-42 at 12-13 (April 2016).

⁸ See NAB Comments at 3. See also Letter from CVCC to Marlene H. Dortch, Secretary, FCC, MB Docket No. 16-42, CS Docket No. 97-80, PP Docket No. 00-67 (May 13, 2016) at 2 (addressing some forms of advertising).

because the structure itself is not grounded in the robust security provided by an MVPD app and its accompanying trust infrastructure. It consequently provides no enforcement tools or financial remedies against third-party manufacturers and developers – capabilities that are built in to MVPD apps deployed today on a wide variety of platforms and devices.

Our experience in standards bodies over many years (including DVB, ITU, MPEG, and ATSC) suggests that it is highly unlikely that standards bodies will be able to develop solutions that meet the requirements set forth in the NPRM, and they will certainly not be able to do so within the limited two-year time frame proposed by the NPRM. Standards processes can be helpful in some cases, but in the case of the dynamic, diverse, and rapidly changing technologies through which commercial video is distributed, it is far more likely that the opening of a standards process will needlessly divert energies. Even if established, those standards would rapidly become obsolete.

As a leader in content creation, production and post-production, with over 100 years' experience in providing technology and creative solutions to the content community, Technicolor is concerned that the proposal creates the potential for unforeseen and unintended consequences downstream and upstream in the content creation ecosystem. We agree with the views of content creators, programming networks, advertisers and the labor community professionals who have warned that by denying content creators the ability to choose to whom they license their works and on what terms, and unfairly shifting revenues from those who take those risks and make those investments to third parties who do not, the proposal would jeopardize the funding and continued creation of programming and harm the millions of labor community members who share directly in downstream revenue.⁹

⁹ See, e.g., Comments of MPAA/SAG-AFTRA; Comments of Content Companies Comments (21st Century Fox, Viacom, A&E Television Networks, CBS Corporation, Scripps Networks Interactive, Time Warner, and The Walt Disney Company).

The NPRM demonstrates little understanding of today's security threats, the nature or need for the security architectures in use today, the adaptive nature of the "bad guy," or how thoroughly the suggested approach would jeopardize security, invite theft of service and jeopardize the creation of programming. Yet the Commission is proposing to redesign the entire architecture that secures all MVPD services and the highest value commercial content without an understanding of or grounding in the realities of security. The proposal in the NPRM would unnecessarily intervene in a dynamic, diverse, and rapidly changing and deny MVPDs the necessary tools and components for commercial success. It should not be adopted.

Respectfully submitted,

/s/ Vince Pizzica

Vince Pizzica
President
Corporate Development and Strategy
Technicolor SA
6040 West Sunset Blvd.
Hollywood, CA 90028