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 THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Rick Chessen
Neal M. Goldberg
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

Paul Glist
Paul Hudson
Davis Wright Tremaine LLP
1919 Pennsylvania Avenue N.W. – Suite 800
Washington, D.C. 20006-3401

May 23, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

I. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED RULES WOULD ASSURE EQUALLY EFFECTIVE PRIVACY PROTECTION FOR CONSUMERS 9

A. Other Laws Do Not Provide Privacy Protection Equal to the Communications Act 10

B. The Proposed Certification Process "Fails to Meaningfully Protect Consumers" 18

II. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED RULES WOULD PROVIDE ROBUST PROTECTION FOR COPYRIGHTED CONTENT 20

A. Content Creators and Owners Are Decisively Opposed to the Proposed Disaggregation Mandate 20

B. The NPRM Proponents Minimize and Distort Content Owners' Serious Copyright Concerns 30

C. Programming Cannot Adequately Be Protected by Litigation 31

D. Programming Cannot Adequately be Protected by Additional Conditions 34

E. Imposition of a Compulsory License Would Be Unwarranted and Unlawful 36

F. The NPRM Proponents Do Not Even Address Protection of MVPDs' or Guide Providers' Copyright Interests 39

III. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED MANDATE IS THE BEST WAY TO PROMOTE CONSUMER CHOICE FOR DEVICES OR CONTENT 41

A. The Promised Benefits of the Proposed Mandate Are Illusory 41

B. There Is Already a "Successor to CableCARD" – Apps Are A Solution and Not a Slogan 50

1. Apps Enable Retail Devices to Use Distinctive Top-Level User Interfaces Without Disassembling a Service Provider's Offering 51

2. MVPD Support for Apps Continues to Expand 53

3. The Functionality of Apps Continues to Expand 57

C. The Proponents Failed to Demonstrate that the Proposed Rules Would Not Jeopardize the Security Of MVPD Services and Networks 60

D. CVCC's Latest Amendments to Its Supposedly "Complete" Proposal Serve Only to Illuminate Its Inherent Flaws 70

1. Proponents' Submissions Continue a Tradition of Constant Changes and Flip Flopping in Technology Proposals. 70
2. The Proposal Is Still a Two-Box Solution 73
3. The Proposal Still Lacks Device Authentication 74
4. The Proposal Makes Device Revocation Even Less Available 75
5. The Proposal Still Rejects World Wide Web Consortium Open IP Standards 75
6. A New Parity Request Cannot Work With the Three Interfaces 76

E. Circular References to Unsupported Assertions Do Not Provide Substantive Record Evidence That a Technical Solution Exists 79

F. The Proposal Continues to Suffer from Unfixable Failings in its Foundation 81

G. No Quick Technical Solution Exists 82

IV. THE PROPONENTS FAIL TO DEMONSTRATE THAT THE PROPOSED RULES ARE A LAWFUL IMPLEMENTATION OF SECTION 629 83

A. STELAR Does Not Grant Any New Authority to the Commission 85

B. The Fact that Equipment Can Include Embedded Software Does Not Make All Stand-Alone Software "Equipment" 86

C. The NPRM Vests Standards Bodies With Too Much Authority 87

V. THE PROPONENTS FAILED TO DEMONSTRATE THAT ADDITIONAL PROPOSED REGULATIONS ARE NECESSARY TO PROTECT CONSUMERS 90

A. No Party Has Offered Any Specific Evidence Demonstrating an Actual Need for Re-Adoption of the Outdated CableCARD Support and Reporting Rules 90

B. Reimposition of the Encoding Rules Is Unnecessary 92

C. There Is No Need to Turn Back the Clock to Rate Regulation 93

CONCLUSION 94

APPENDIX A – A TECHNICAL ANALYSIS OF THE MULTIPLE "COMPETITIVE NAVIGATION" PROPOSALS
Ralph W. Brown

APPENDIX B – SELECTION OF PROGRAMMER APPS

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 THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] submits these reply comments in response to the public comments filed in response to the Notice of Proposed Rulemaking ("NPRM")[2] in the above-captioned proceedings.

The NPRM drew far more opposition, from a much wider variety of parties, than it did support. Serious concerns with the proposed rules were raised by studios, networks, independent and diverse content creators, directors, writers, record labels, small and large service providers, device manufacturers, legislators, and nationally-respected advocates of consumer privacy, disability access, diversity, energy efficiency, commerce, intellectual property, innovation, and labor. From every direction, it is evident that the Commission's proposal is not as simple as the

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 80 percent of the nation's cable television households, more than 200 cable program networks, and others associated with the cable industry. The cable industry is the nation's largest provider of broadband service after investing over $245 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to approximately 30 million customers.

[2] Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices, Notice of Proposed Rulemaking, MB Docket No. 16-42, 18 Fed. Reg. 14033 (Mar. 16, 2016) ("NPRM"); *Media Bureau Announces Comment and Reply Deadlines for Video Navigation Choices NPRM and Establishes Schedule for Ex Parte Meetings*, Public Notice, MB Docket No. 16-42 (Mar. 17, 2016) (extending comment deadline by seven days to April 22, 2016).

NPRM portrays,[3] and that its adoption would leave a long trail of unintended negative consequences in its wake.

When the Commission considered the imposition of a less-invasive tech mandate a decade ago, the broadcast flag, it received similar warnings about the unintended consequences of attempting to regulate through detailed technical prescriptions in a rapidly-changing market: "[H]eavy-handed 'tech mandates'" would "inject[] government into technological design" and "set[] in stone" specific technical requirements "for technologies that are constantly changing." The Commission was urged instead to rely on "technological tools developed in the marketplace, not mandated by government," since it "has neither the resources nor the expertise" to engage in "dictating the marketplace for all kinds of electronics." "This type of government oversight of technology design will slow the rollout of new technologies and seriously compromise US companies' competitiveness in the electronics marketplace," since government-imposed "[t]echnology mandates … limit[] both innovation and consumer choice while increasing costs to innovators and consumers." "The market for delivering content digitally over new technologies is working. Consumers can watch and listen to the content they purchase anytime and anywhere they want. … All of these great developments happened without government intervention," which shows that "government intervention in the free market [in this case is] unnecessary."[4]

That critic was Public Knowledge, now one of the proponents of the NPRM's proposed set-top box technical mandate. While the then-Commission ignored their advice, the D.C.

[3] As Commissioner Rosenworcel has observed, "This rulemaking is complicated. …The most successful regulatory efforts are simple ones. More work needs to be done to streamline this proposal." NPRM, Statement of Commissioner Jessica Rosenworcel.

[4] Gigi B. Sohn, Don't Mess with Success: Government Technology Mandates and the Marketplace for Online Content, 5 J. ON TELECOMM. & HIGH TECH. L. 73, 75-76, 83 (2006-07).

Circuit vacated the broadcast flag rule as beyond the Commission's authority, and Public Knowledge's prediction of market successes unshackled by technical mandates came true.[5]

The current Commission should not make the same mistake again. Those urging the Commission forward are relying on baseless talking points, fallacies, and demonstrably defective technology claims which, however often repeated, still provide no basis for adopting the proposed rules. Reliance on proponents' unsupported assertions would be arbitrary and capricious. There is still time for the Commission to hit the pause button and seek out better, and simpler, ways to assure that consumers have access to competitive retail devices to access the video services that they purchase from MVPDs, without stealing the value of content from its creators, jeopardizing the security of MVPD services and systems, crippling the ability of MPVDs to protect their customers' privacy, skewing the market by effectively prohibiting MVPDs (but not OVDs) from meeting consumer demand for boxless app solutions, and violating the Communications Act, the Copyright Act and the Constitution.

EXECUTIVE SUMMARY

The Commission's proposal for radical intervention in the video marketplace has now met an outpouring of condemnation.

The Proposal Sacrifices Consumer Privacy

Privacy advocates have agreed that the FCC's proposal to deny consumers their statutory privacy rights under the Communications Act and replace them with unenforceable self-certification is "inconsistent with [] reality." Democratic and Republican co-chairs of the Congressional Privacy Caucus have agreed. The Federal Trade Commission has no authority or ability to provide equivalent protections. Google has already told the courts that "Google is not a

[5] *American Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005).

video tape service provider" under the federal videotape law that the NPRM suggests could provide adequate privacy protections, and State laws are no substitute. NTIA has admonished "the baseline privacy protection a subscriber receives should not hinge on where the consumer lives."

The Proposal Undermines Copyright

Creators of content have explained how the proposal violates the rights enshrined in the Copyright Clause of the Constitution. Studios, networks, independent and diverse content creators, music providers, and intellectual property scholars have demonstrated that granting a "zero-rate compulsory license" for commercial exploitation of their works by unlicensed third parties violates the "ability to choose whom to license their works to and on what terms," which "is a key component of copyright owners' property interests." The Commission has no authority to grant a new compulsory license, nor is one required: licenses to provide video content on retail devices have already been negotiated by more than 115 legitimate online sources, including Netflix, Hulu, Amazon, Sony PlayStation Vue, Sling TV, Verizon go90, and AT&T's three new DIRECTV online offerings.

Organizations representing more than 1.8 million labor community members have weighed in against the proposal. DGA, IATSE, and SAG-AFTRA[6] have warned that the FCC's proposal "will cause substantial economic harm" not only to the content creators but also the hundreds of thousands of workers employed by the content industry "because our members share directly in the downstream revenue" earned by copyrighted content. IBEW and CWA[7] have warned against the damaging impact on service delivery and customer service.

[6] The Director's Guild of America, the International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada, and The Screen Actors Guild-American Federation of Television and Radio Artists.

[7] International Brotherhood of Electrical Workers and the Communications Workers of America.

Minority-owned and independent programmers and diversity advocates also oppose the NPRM by an overwhelmingly wide margin, with most citing grave concerns about misappropriation of their content and violation of their license terms. "The loss of the negotiated right to particular placement – a very difficult right to secure for a diverse programmer – would cause particular harm to TV One and other minority programmers."

The Association of National Advertisers has explained how the proposal "would also unfairly shift advertising revenues from those who invest in, and take considerable risks in, creating the programming, to third parties who seek to build their businesses on content they have not licensed."

Over 150 members of Congress have challenged the Commission's approach, including copyright experts on the Judiciary Committees and over half of the members of the House Democratic Caucus.

In response, proponents suggest that copyright owners could litigate their claims individually against each specific infringement. But as MPAA explains, the primary mechanism for copyright holders to enforce their exclusive rights are the licensing and distribution agreements that program producers use to license content to networks and that networks use to window, segment, and define the economic terms for distribution among various broadcast, MVPD, and online distributors: "content owners do not make primary use of litigation in the marketplace in order to enforce and protect their rights." The FCC's circumvention of the technological protection measures protected by the DMCA is unlawful and destructive of the video marketplace.

There Is No Need for the Proposed New Rules in Today's Market of Unprecedented Choice

Most tellingly, proponents have not answered the question best posed by sixty members of Congress, who recently asked the Commission "what purpose the new rules would serve in this era of unprecedented consumer choice." The market has already developed apps as the "successor to CableCARD" that fulfills the goals of Section 629(a). Powerful incentives have propelled MVPDs to develop, support, and continue to expand apps even beyond the 460 million retail devices already supported. Apps power the successful market in which consumers are buying retail devices and accessing MVPD and OVD content; even the smallest independent producer or programmer can successfully disseminate its content to millions of consumers; and integrated search is developing organically right now. Apps can be updated rapidly. And apps reduce MVPDs' capital expenditures, maintenance costs, truck rolls and installation visits, thus reducing costs to consumers. Rather than building on the success of the apps-based model that maps the path away from set-top boxes, an FCC set-top box mandate won't eliminate the box – technologically, it will lock in the box. Nor can the NPRM deliver on a vision of a world of seamless navigation around online and MVPD content, because it unbundles only MVPD content and does not require the disaggregation, search, or any other unlicensed use of OVD content. As to claims that the FCC mandate will somehow aid small systems and promote new facilities-based broadband networks, the operators of such systems have demonstrated the opposite and oppose the proposal.

The Proposal Jeopardizes Security

The proposal to release content without the licenses, privity, applications and technologies that secure the distribution of commercial video would jeopardize security and abet,

rather than prevent, theft of service. Chairman Wheeler has sought to mask this failure of security by simply claiming without any support that delivering content "safely" to a third-party device *with an MVPD app* and inside the trust infrastructure "is proving our point" that you can do so *without an MVPD app* and outside that trust infrastructure and not suffer "all these other horrible things" like loss of privacy, copyright, and security and eroding the economic foundation for television. But the technical evidence and record is clearly to the contrary.

Proponents of the NPRM offer proposals that would only worsen security. They would artificially narrow security options still more, advertise common points of attack, and undercut any means for verifying that a user or device is authorized to receive service. These proposals would violate Congress's command in Section 629(b) that the FCC "shall not prescribe regulations … 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."

CVCC's latest amendments to its supposed technical solution carry on its long tradition of constant changes and flip flops in technology proposals, and only serve to illuminate that it has no working solution for the NPRM. Its new version does, however, answer the two-box question: *it requires a second device* in the home. Its proposal for authenticating users raises even more concerns about security and would create an easy path for pirate boxes to access MVPD content. In addition, CVCC further waters down an already useless self-certification regime to slow or stop any revocation of non-compliant devices.

The Proposal Exceeds Legal Bounds

Rather than advancing any serious legal defense of the NPRM, proponents grasp at straws.

STELAR did not grant any authority to the Commission beyond receiving a DSTAC Report. It certainly did not call for a new technology mandate or for an NPRM diametrically opposed to the "technology and platform neutral" directive from Congress.

Nor does the presence of embedded software and other operating systems in navigation device hardware magically transform the entire universe of other unrelated software applications into navigation device equipment.

Far from "consulting" with standards bodies, the FCC would authorize them to legislate binding federal requirements without legal accountability. To this, proponents now add equally lawless requests to "stack" the vote against MVPDs and content providers in those standards bodies. This entire effort violates constitutional principles that preclude vesting unaccountable bodies with the power to legislate, and clear prohibitions against agencies putting regulation into the hands of an industry's rivals.

Rather than producing any record to justify intervention, the NPRM has yielded an overwhelmingly one-sided condemnation of the proposal it pushes and a correspondingly substantial record demonstrating that the apps-based approach avoids all the harms of the NPRM's proposal. In the face of such a record, continued pursuit of the NPRM's proposal would be arbitrary and capricious.

There Is No Need for Additional CableCARD Rules

No party offered any specific evidence demonstrating an actual need for re-adoption of the outdated CableCARD support and reporting rules. Nor has TiVo provided any basis for reimposing the very encoding rules vacated by the DC Circuit. There is no evidence that MVPDs have been arbitrarily encoding content to disadvantage retail devices, which was the animating concern and basis for adopting encoding rules in the first place. But adopting those

rules would distort the market: a content provider that wanted to offer secure streaming of early release content could use TiVo or an online video provider, but would have to seek a waiver if it wanted to pursue a similar model with an MVPD.

The only clear result of adopting the suggested transparency rules would be to prohibit MVPDs from continuing to benefit consumers with free or deeply discounted set-top boxes.

I. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED RULES WOULD ASSURE EQUALLY EFFECTIVE PRIVACY PROTECTION FOR CONSUMERS

Numerous commenters agreed with NCTA that the NPRM's proposed rules threaten consumers' statutory privacy rights and expectations under the Congressionally-mandated protections and remedies set forth in Sections 338(i) and 631 of the Communications Act.[8] Retail device manufacturers and app developers would be able to capture details of individual consumers' television viewing data and then use or sell that data to insert personally-targeted ads to follow consumers and their children around the television and beyond, free of the restrictions on the use of consumer's private information that apply to MVPDs under the Communications Act. Google, which has built its business by exploiting consumers' personal information, tells the FCC that there is nothing it can do about that: "limitations on the FCC's jurisdiction under Section 629 of the Communications Act prevent it from applying the rules that apply to 'cable operators' and 'satellite carriers' to suppliers of devices."[9]

---

[8] *See, e.g.*, AT&T Comments at 48-53, 82-86; Comcast Comments at 25, 93-97; Communications Workers of America (CWA) Comments at 4-5; Digital Citizens Alliance Comments at 12; Electronic Privacy Information Center (EPIC) Comments at 3-7; Free State Foundation Comments at 2-3, 12-13; Frontier Comments at 14-15; International Center for Law & Economics Comments at 10, 31, 35; ITTA Comments at 17-20; Midcontinent Comments at 3; Multicultural Media, Telecom And Internet Council (MMTC) *et al*. Comments at 19-21; Taxpayers Protection Alliance Comments at 4-5; United States Telecommunications Association Comments at 12-15.

[9] Google Comments at 7. By contrast, Public Knowledge suggests that "a competitive device may be viewed as part of a 'cable system' under 47 U.S.C. § 522 … and thus come under [the Communication Act's] direct authority." Public Knowledge Comments at 36.

Google claims that "new privacy rules specifically directed to new generations of devices and applications [are] *unnecessary*" because the Commission can instead rely on a patchwork of FTC enforcement and state laws.[10] Amazon similarly claims that the new gap in coverage of Sections 338 and 631 "would not present significant consumer privacy concerns" because the FTC enforcement offers "equally effective privacy protection" to the Communications Act,[11] and TiVo also urges the FCC to rely on FTC and state enforcement.[12] Chairman Wheeler has hewed to the talking point that self-certification and FTC authority should be sufficient to protect subscriber privacy. In fact, the proposal opens gaping holes in consumer privacy that none of these patches can fix.

A. Other Laws Do Not Provide Privacy Protection Equal to the Communications Act

Privacy advocates with no stake in the navigation device market reject Google, Amazon, and the Commission's contentions. The Electronic Privacy Information Center (EPIC) says the FCC's view that there is no cause for concern is "inconsistent with [] reality,"[13] noting that even in today's limited retail market, TiVo and others have used private information in excess of what would be permitted by cable operators.[14] Contrary to Amazon's contention that it is already subject to "equally effective privacy protection requirements," NTIA comments that "MVPDs

[10] Google Comments at 7 (emphasis added).

[11] Amazon Comments at 7. Amazon acknowledges that the "privacy regime under the Communications Act" would not apply to "competitive providers of navigation devices," and TiVo notes that its "retail devices are not subject to Section 631 because TiVo is not a MPVD." TiVo Comments at 25.

[12] TiVo Comments at 25-28. TiVo also argues that "[t]he Cable Privacy Act restricts the *disclosure* of personally identifiable viewing information without consent. It does little to restrict the *use* of such data by MVPDs. Cable operators are free to use set-top box data to target advertising, perform analytics, or combine it with other sources of data which they are doing more and more extensively. … allegations that "tech companies" will be able to make more intrusive use of set-top box data than MVPDs are doing today are inaccurate." TiVo Comments at 30 (emphasis in original). Under Section 631, cable companies can only use data with customer notice and consent, and if they fail to comply with these restrictions, the customer has a right to bring private legal action in federal court. A cable customer using a retail device would not be guaranteed these safeguards.

[13] EPIC Comments at 5.

[14] *Id*. at 5-6.

generally have more rigorous statutory obligations concerning their collection and use of personally identifiable subscriber information than do non-MVPD providers of navigation equipment," and exhorts that the FCC needs to "take steps to ensure that expansion of competition in navigation devices does not diminish existing privacy protections for multichannel video programming subscribers."[15]

The Democratic and Republican co-chairs of the Congressional Privacy Caucus wrote to the Chairman to express their "concern that existing privacy protections enjoyed by cable and satellite subscribers will not be retained" under the NPRM's proposed rules, and that "[h]owever the Commission chooses to go forward, its actions cannot result in a loss of privacy protections, customers' loss of service through no fault of their own or that of an MVPD [which they note could occur if an MVPD shut off service to all users of a device found to be in violation of the FCC's proposed self-certification requirement], or customers' private right of action against violators."[16] The Digital Citizens Alliance objected to the rules as proposed, saying that the FCC needed to "take meaningful steps to protect consumer expectations of security and privacy prior to authorizing a set of enhanced, interconnected, and potentially vulnerable devices capable of collecting sensitive personal information from everyone in the home, including children."[17] The Communications Workers of America decried that the gap in privacy protection that would be created by the NPRM would allow "third parties to data-mine consumer viewing habits and other personal information without getting permission from the consumer and without paying for the

[15] National Telecommunications and Information Administration (NTIA) Comments at 5.

[16] Letter from Rep. Joe Barton and Rep. Diana DeGette, Congressional Privacy Caucus, to Hon. Tom Wheeler, Chairman, FCC (May 11, 2016); *see also* Amir Nasr, *Capitol Hill Unrest Over FCC Set-Top Box Proposal Heats Up*, MORNING CONSULT (May 12, 2016) (discussing Congressional Privacy Caucus letter).

[17] Digital Citizens Alliance Comments at 5-6.

video content that gives them access to this consumer data."[18] And Jeff Chester of the Center for Digital Democracy stated, "It's outrageous that as Google expands the data it collects for targeting video advertising, it opposes having the FCC ensure through stronger rules that set-top boxes ... can actually protect consumer privacy."[19]

Google dominates the search market[20] and monetizes consumer data collected not just from that search engine but from Chrome, Maps, Mobile, Blogs, Picasa, Wallet, YouTube, Cloud, Google Plus, Google Fiber, Gmail users and their non-Gmail correspondents to fuel its massive advertising business.[21] Google's privacy practices have repeatedly fallen short of requirements.[22] There should be no doubt that as Google accesses the private television viewing data exposed under the proposed rules, consumers will again find themselves confronted with even more privacy affronts[23]—but no meaningful remedy under the Commission's proposed approach.

---

[18] CWA Comments at 4.

[19] Jacob Kastrenakes, *Google Opposes New Privacy Protections for Set-Top Boxes*, THE VERGE (Apr. 26, 2016), http://www.theverge.com/2016/4/26/11511988/google-opposes-set-top-box-privacy-protection-expansion-fcc-filing.

[20] *See Share of Search Queries Handled by Leading U.S. Search Engine Providers as of January 2016*, STATISTA, THE STATISTICS PORTAL (last visited May 19, 2016), http://www.statista.com/statistics/267161/market-share-of-search-engines-in-the-united-states/ ("Market leader Google generated 68.8 percent of all core search queries in the United States and accounted for 89.3 percent of the global search market as of mid-2015.").

[21] *See* Comcast Comments at 95 (noting that Google's "entire business model is based on collecting, using, sharing, and monetizing huge amounts of consumer data for advertising and other purposes"); AT&T Comments at 49 (discussing "the troves of information [Google] already collects regarding the thoughts, interests, concerns, plans, locations, and movements of hundreds of millions of specific individuals"); Robert Hof, *Google's Ad Machine Is Even More Profitable Than Anyone Knew*, FORBES (Feb. 1, 2016), http://www.forbes.com/sites/roberthof/2016/02/01/googles-ad-machine-is-even-more-profitable-than-anyone-knew/#1debfed07e7a (noting that investors "focused on better-than-expected revenues and profits thanks completely to Google's massive advertising business. Ad revenues rose 17 percent, to $19.1 billion.").

[22] *See* NCTA Comments at 82-83 (enumerating various fines, investigations and controversies spawned by the privacy practices of Google and others, including a record FTC fine for bypassing browser settings).

[23] *See, e.g.*, AT&T Comments at 50 ("Because of the volume and diversity of data that Google retains – its "data dominance" – it would be uniquely able to provide targeted advertising to video customers (as well as users of its other services).").

Whether or not the Commission rejects Google's reflexive resistance to privacy restrictions, the privacy gap created by the Commission's proposal cannot be bridged by self-certification and Federal Trade Commission ("FTC") enforcement. While the FTC might generally have a role to play when privacy promises are broken, the Commission is not requiring third parties to match the specific promises that cable and satellite providers make and the specific choices they provide to their subscribers as part of their specific service. The NPRM proposes that third parties need only self-certify that they "will adhere to privacy protections."[24] Section 631 confers upon individual consumers a right to bring a private legal action to enforce the requirements of Section 631 and the commitments of cable and satellite providers. There is no basis to expect the FTC to take enforcement action for one injured citizen, nor does it have authority to award private damages or to create a consumer's private right of action,

Section 631 also protects consumers by requiring that if government agencies or law enforcement seeks personally identifiable viewing records, the consumer first receives notice and an opportunity to contest, and the government must obtain a court order after presenting clear and convincing evidence that the subscriber is engaged in criminal activity.[25] The FTC cannot provide this same protection, and there is no basis for assuming that law enforcement will voluntarily adhere to these higher statutory protections before demanding and accessing viewing data from third parties who are not bound by the specific protections promised to subscribers in

[24] NPRM at ¶ 73.

[25] In prior rulings, the FCC has recognized that Section 631 cannot be construed or administered in a manner that negates the court order requirement for government access to viewing data. In a 1992 order rejecting efforts to compel release of cable company complaint records to local governments through FCC rule, the FCC explained that such an approach "might negate the separate court order requirement that would otherwise limit governmental access to this type of information. This does not appear to have been intended." *Cable Television Technical and Operational Requirements; Review of the Technical and Operational Requirements of Part 76, Cable Television*, Memorandum Opinion and Order, 7 FCC Rcd. 8676 ¶ 39 (1992).

the Communications Act, nor do they have the legal ability provided to MVPDs to refuse requests that do not meet that statutory bar.

While all MVPDs subject to Section 631 have a presence in the United States, the FTC may be unable to reach foreign device manufacturers and app developers. And it remains the case that the NPRM provides no contractual or technical tools for determining what data the third party – foreign or domestic – is collecting, how it is using the data, or whether it is unlawfully sharing it with other parties.

Privacy critics have thoroughly demonstrated that the possibility of an FTC or state enforcement action is no "equal" substitute for the pervasive Communications Act protections that consumers can choose to enforce directly in federal court. EPIC explained that "[s]uggestions that the FTC would enforce privacy self-certifications provide little reassurance to consumers, as this agency rarely enforces the terms of its settlement agreements with privacy violators."[26] And earlier this month, a senior FCC official cautioned that the FCC should not rely on the FTC to protect consumer privacy in communications services, stating that the FTC has always had challenges in "understanding what's going on" with telecommunications service issues and "having visibility into practices."[27]

There is also a fundamental legal flaw in enlisting the FTC to enforce Communications Act privacy provisions. The FCC has accepted the view of device manufacturers and app developers that they are not "cable" or "satellite" under the Communications Act, and has stated unequivocally and repeatedly that "it has no intent to regulate edge providers" privacy

[26] EPIC Comments at 7.

[27] Jimmy Hoover, *FCC Official Says Privacy Plan Won't Stifle ISP Marketing*, LAW360 (May 2, 2016), http://www.law360.com/articles/791368/fcc-official-says-privacy-plan-won-t-stifle-isp-marketing.

practices.[28] That gap cannot be cured by having the FTC attempt to enforce a self-certification scheme under Section 5 of the FTC Act. The FCC has no authority to sub-delegate its enforcement responsibilities to another federal agency without authorization from Congress.[29] Congress knows how to authorize inter-agency delegations,[30] and it did not do so in Section 631. None of the examples of compliance certification enforcement cited by the FTC's Director of the Bureau of Consumer Protection include any comparable instance in which the FTC has undertaken widespread enforcement of a promise to comply with a Congressional statute.[31] Such sub-delegation would be particularly inappropriate where, as here, the FCC has no authority to regulate device makers and app developers under Section 631 in the first place, and the entire scheme would be a patent effort to avoid those limits.[32]

Even proponents of the NPRM like the Digital Media Association concede that "the legal framework that [would] appl[y] to would-be new entrants to the navigation device market is

---

[28] *Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor Do Not Track Requests*, RM-11757, 30 FCC Rcd 12424 ¶ 1 (Nov. 6, 2015).

[29] *See, e.g., U.S. Telecom Ass'n v. FCC*, 359 F.3d 554, 565-66 (D.C. Cir. 2004) ("[T]he cases recognize an important distinction between subdelegation to a *subordinate* and subdelegation to an *outside party*. . . . We therefore hold that, while federal agency officials may subdelegate their decision-making authority to subordinates absent evidence of contrary congressional intent, they may not subdelegate to outside entities—private or sovereign—absent affirmative evidence of authority to do so."); *G.H. Daniels III & Assocs. v. Solis*, 626 F. App'x 205, 207 (10th Cir. 2015) ("Courts are quite tolerant of the administrative practices of agencies, but passing the buck on a non-delegable duty exceeds elastic limits.").

[30] *See, e.g.*, 31 U.S.C. § 3726(g) ("The Administrator may delegate any authority conferred by this section to another agency or agencies if the Administrator determines that such a delegation would be cost-effective or otherwise in the public interest.").

[31] Comments of Jessica L. Rich, Director of the Bureau of Consumer Protection, Federal Trade Commission.

[32] The FTC lacks independent authority to interpret or enforce the Communications Act. The Act specifically references the particular instances in which the FTC has a role to play – none of which makes any mention of Section 631. *See* 47 U.S.C. §§ 228(c)(1), (3), (10), 313. Because the FTC has not been entrusted with implementing the Communications Act, it may not authoritatively interpret or enforce it. Nor is the Director of the Bureau of Consumer Protection empowered to speak on behalf of the FTC as a whole.

different from the one that currently applies to MVPDs."[33] And those differences include deficiencies that the FCC cannot bridge if it also sticks to its proposed disaggregation mandate.

The NPRM asked whether the Commission could rely upon the Video Privacy Protection Act (VPPA) to protect the privacy of consumers using retail devices.[34] EPIC has described VPPA as a law that "primarily prevents disclosure of personally identifiable rental records of 'prerecorded video cassette tapes or similar audio visual material'" and "is not often invoked."[35] In its initial comments, NCTA explained that the Commission cannot rely on VPPA,[36] and in their comments neither Google, CVCC, Amazon, nor Public Knowledge support application of the VPPA as they once did in *ex partes*.[37] Google has previously convinced courts that the VPPA does not apply to it,[38] and just this month reiterated to the Third Circuit Court of Appeals that it "cannot be held liable under the VPPA because Google is not a video tape service provider."[39] Whatever the final outcome of debates over VPPA,[40] it clearly cannot today be deemed a viable replacement for Section 631 to protect the privacy of consumers using retail devices to access their cable programming.

---

[33] Digital Media Association Comments at 6.

[34] NPRM at ¶ 78; *see also* NCTA Comments at 84.

[35] *See Video Privacy Protection Act*, EPIC.org Privacy by Topic: The A to Z's of Privacy (last visited May 12, 2016), https://epic.org/privacy/vppa/.

[36] *See* NCTA Comments at 84.

[37] *See* Letter from Consumer Video Choice Coalition (CVCC) to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Jan. 27, 2016) at 4 ("Competitive offerings may also be subject to the Video Privacy Protection Act.").

[38] *See* NCTA Comments at 84 (citing *In re Nickelodeon Consumer Privacy Litigation*, 2014 WL 3012873 (D.N.J. July 2, 2014)).

[39] Defendant-Appellee Google Inc.'s Rule 28(j) Response to Submission of *Yershov v. Gannett Satellite Info. Network, Inc., d/b/a USA Today*, No. 15-1719, --- F.3d ---, 2016 U.S. App. LEXIS 7791 (1st Cir. Apr. 29, 2016) as Supplemental Authority, In re Nickelodeon Consumer Privacy Litig., No. 15-1441 (3rd Cir. May 6, 2016).

[40] *See, e.g., Yershov v. Gannett Satellite Information Network, Inc.*, Slip Op., No. 15-179 (1st Cir. Apr. 29, 2016) (noting controversies involving the scope and applicability of the statute).

Calls to rely on state laws fail for similar reasons.[41] In any event, trying to do so would contravene Congress' decision to create national privacy protections for all MVPD customers and NTIA's admonishment that "the baseline privacy protection a subscriber receives should not hinge on where the consumer lives."[42] That would not be the only bizarre result from the Commission's reliance on such a patchwork of incomplete remedies and safeguards; because many consumers may use both retail and MVPD-leased devices, some consumers would have different privacy protection regimes, and remedies, depending on what device they are using in different rooms in the same house!

CVCC also claims that privacy concerns can be protected by the "competitive market," which it claims "will allow consumers to choose between different providers, in part based on their different privacy policies."[43] INCOMPAS similarly contends that "consumers will drive developers to institute robust privacy policies"[44] – a confidence not shared by many privacy advocates, NTIA, or Congressional privacy experts. In any event, Congress has decided that cable subscribers should receive statutory and enforceable privacy protection under the Communications Act, and the FCC has no authority to carve exceptions into that law.

[41] The cable privacy law in Google and TiVo's home state of California only applies to "cable" and "satellite," and they say they are neither. California Penal Code § 637.5. The California Online Privacy Protection Act does not provide a right to bring private legal action and clearly does not protect most American consumers. Most states do not have laws that even partly cover the protections afforded by the Communications Act. Although Google advises the Commission that fraud and deceptive practices under state law can serve as a privacy substitute, such general consumer protection statutes are no substitute. As with the VPPA, the message outside of the FCC is the opposite. Google has refused to comply with Mississippi Attorney General Jim Hood's efforts to use general statutes to even investigate its protection of commercial video content.

[42] NTIA Comments at 6, n.27.

[43] CVCC Comments at 44.

[44] INCOMPAS Comments at 23.

B. The Proposed Certification Process "Fails to Meaningfully Protect Consumers"

EPIC thoroughly demonstrated that the FCC's proposed band-aid fix, requiring retail providers to self-certify their voluntary compliance with privacy protections, "fails to meaningfully protect consumers."[45] EPIC explained that the NPRM's "proposal fails to provide for effective oversight and enforcement, and instead appears to deputize cable companies to enforce privacy rules on retail device manufacturers."[46] Continuing, EPIC cautioned that, "Significantly, the proposal lacks clarity on whether the FCC could bring an enforcement action against device manufacturers for false certifications or violations of the Cable Subscriber Privacy Rules."[47] NTIA says that the certification proposal "leaves important questions to be addressed – most importantly, who will ensure compliance with a certification and through what legal authority."[48]

The answer to NTIA's important question is that *no one* will be able to ensure compliance. The FCC cannot create a replacement cause of action. Moreover, it will often not be possible for MVPDs to detect violations,[49] or to selectively terminate violators when they do. And even if the MVPD could cut off access to a device or app, now CVCC wants that process to be further protracted by a mandatory mediation process, during which time the offending device

[45] EPIC Comments at 7. *See also* NCTA Comments at 78-81; AT&T Comments at 84-85, Comcast Comments at 92-100.

[46] EPIC Comments at 7.

[47] *Id*. at 7.

[48] NTIA Comments at 5.

[49] CVCC's suggestion (at 43-44) that certifications could be provided electronically does nothing to assist the MVPDs' ability to enforce compliance; it would merely change the medium by which unreliable promises are delivered. It would be easy for a non-compliant device to spoof the URL for a compliant device from another manufacturer in the HTTP header. *See* Ralph W. Brown, A Technical Analysis of the Multiple "Competitive Navigation" Proposals at 13, attached as Appendix A ("Technical Analysis").

or app could continue to abuse and misuse consumers' private information.[50] It would be difficult to design a less effective regime.

* * *

In sum, none of the NPRM proponents offer an actual solution that would assure that consumers receive "equally effective privacy protection" to the Communications Act. The reason for this is plain. There *is* no lawful means for the Commission to fully replace the protections of the Communications Act and still implement its disaggregation mandate. The Commission cannot jettison the unambiguous privacy protections provided by Congress in Sections 338 (i) and 631[51] in favor of its tortured reading of Section 629. Indeed, to the extent that Section 631 and 629 represent competing imperatives – which is the case here *only* as a result of the NPRM's strained construction of Section 629 – the Commission is making the wrong trade-off. The Consumer Federation of America (CFA) agrees, explaining that Commission policies "adopt[ed] under other sections of the Act must not be undermined by [pursuit of] competition in the set-top box market," and, further, that its support of the NPRM is contingent on the assurance that "viewers who utilize third-party set-top boxes [will] have the *same* privacy protections as those who use cable operator-owned set-top boxes."[52] Absent that assurance, the CFA urges that "other sections will take precedence [over Section 629], which is clearly what Congress intended."[53]

As NCTA explained in its comments, if the FCC relied on apps to address its Section 629 mandate instead of its disaggregation approach, privacy could be better protected through

[50] CVCC Comments at 43 (proposing to forbid service interruption for lengthy "cure" and dispute resolution process).

[51] 47 U.S.C. § 338(i) applies § 631 privacy obligations to satellite.

[52] Consumer Federation of America (CFA) Comments at 13 (emphasis added).

[53] *Id*.

agreements and security chains of trust, as it is currently. The Digital Citizens Alliance astutely quotes Professor Dan Wallach of Princeton University, commenting that "the deeper issue [underlying privacy protection] is that 'it's relatively easy to build something that works, but it's significantly harder to build something that's secure and respects privacy.'"[54] That is what the MVPDs have done with apps, and the Commission ought to be building upon that success, rather than discarding it in favor of a clearly ineffective regime that would expose consumers to willful and repeated violations of the privacy expectations that Congress expressly granted them, with little or no opportunity for remedy.

II. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED RULES WOULD PROVIDE ROBUST PROTECTION FOR COPYRIGHTED CONTENT

A. Content Creators and Owners Are Decisively Opposed to the Proposed Disaggregation Mandate

While professing to leave copyrights and distribution licenses intact, the proposed rules would compel distribution of programming for commercial exploitation by unlicensed third parties that disavow responsibility for abiding by any licensing obligations or the need to be subject to any enforceable FCC rules. NCTA warned in its comments that such a framework would undermine the copyright and licensing protections that are necessary to sustain high-quality programming.[55] The record now clearly confirms that warning, as evidenced by the widespread outcry from content creators and their supporters that filed comments opposing the proposed rules, and by the comments of the NPRM's proponents that do not disavow the objectives they stated in DSTAC to disregard the terms of the content owners' licensing agreements.

[54] Digital Citizens Alliance Comments at 8.

[55] NCTA Comments at 31.

TiVo urges the Commission to move forward in allowing retail providers to ignore and violate programming agreements: "it makes no sense for competitive device providers to have to adhere to licensing terms that they have no way of knowing and which would vary drastically across MVPDs."[56] Numerous comments from supporters of the proposed rules explicitly acknowledge that retail providers would repudiate license agreements.[57] The proponents' comments give some lip service to protection of copyright and programming licenses, such as Amazon's comment that the "intellectual property of programming content and business agreements can and must be protected."[58] But while Public Knowledge claims that "the interests of copyright holders are aligned with the Commission's proposal,"[59] the copyright holders demonstrate the opposite.

Licensing. The joint comments of the "Content Companies" (including many of the world's largest and most prominent networks and studios: 21st Century Fox, Viacom, A&E Television Networks, CBS Corporation, Scripps Networks Interactive, Time Warner, and The Walt Disney Company), explain that, "[b]y inviting third parties to aggressively seek to profit from the Content Companies' investments without incurring any of the obligations that effectively safeguard and thereby promote the creation of valuable programming today, the Commission's proposal reduces the incentives to continue to create the great programming that

---

[56] TiVo Comments at 19.

[57] *See, e.g., id.* at ii (cannot be bound by programming agreements); Public Knowledge Comments at 12, 45-46 (dismissing license conditions as "legally ineffective" and asserting that "a device manufacturer should be able to access linear MVPD programming without needing to negotiate with major programmers" and then providing "flexible and varied ways" for consumers to "access and interact with content."); INCOMPAS Comments at 5 (seeking to provide an integrated user interface that would blend programming from their MVPD and programming available on the Internet); Letter from CVCC to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Jan. 21, 2016) at 4 ("Makers and marketers of competitive devices cannot be expected to respect private, secret, and temporary pacts between and among MVPDs and content owners."). TiVo's CTO admitted at an industry conference that third party device makers would be able to interfere with the advertising embedded in the data streams "unlocked" by the FCC's mandate. *See* NCTA Comments at n.106.

[58] Amazon Comments at 5.

[59] Public Knowledge Comments at 10.

consumers enjoy," and would "upend the video marketplace in ways destined to harm content creators and consumers, while providing unwarranted benefits to app and technology developers with little or no appreciable benefit to the public interest."[60]

Similarly, the Motion Picture Association of America and the Screen Actors Guild-American Federation of Television and Radio Artists, as the representatives of the nation's movie studios and approximately 160,000 industry professionals, condemned the NPRM because it "explicitly refuses to prohibit third parties from improperly manipulating content, including altering channel lineups and advertising, even though programmers and MVPDs extensively negotiate terms on content presentation in their licensing agreements," and it "interferes with the ability of copyright holders to negotiate content protection terms, jeopardizing the security of their programming and impeding their legal rights to prevent theft."[61] MPAA and SAG-AFTRA warned that the NPRM's proposal threatened to undermine the economics of content creation, an industry that contributed $131 billion in sales to the overall economy in 2014 and is one of the nation's brightest sectors in generating positive balance of trade.[62]

The Director's Guild of America and the International Alliance of Theatrical Stage Employees, Moving Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada (IATSE) wrote that to "open set-top boxes to services that engage in trafficking illegal content, have no respect for copyright, and even less willingness to compensate those who create films and television programs," "with no licensing and contractual obligations," "will cause substantial economic harm" not only to the content creators but also the

[60] Content Companies Comments at iii-iv.

[61] MPAA/SAG-AFTRA Comments at ii.

[62] *Id*. at ii, 3.

hundreds of thousands of workers employed by the content industry "because our members share directly in the downstream revenue" earned by copyrighted content.[63]

Minority-owned and independent programmers and diversity advocates also oppose the NPRM by a wide margin, with most citing grave concerns about misappropriation of their content and violation of their license terms.[64]

CreativeFuture, a coalition of 450 companies and organizations and over 60,000 individuals employed in creating content, protests that the FCC's proposal "would allow

---

[63] Director's Guild/IATSE Comments at 2-3, 5.

[64] *See, e.g.,* MMTC *et al.* Comments at 3 (remarking that the proposed rules would "harm diverse programmers and content creators by violating their copyright and licensing agreements and existing distribution arrangements with MVPDs, the lifeblood of their very existence"); National Urban League *et al.* Comments at 1 (requesting that the Commission "hit the 'pause' button on this proceeding"); Hispanic Leadership Fund Comments at 1 (expressing "concern[] that this rule appears likely to slow or reverse the progress that Hispanic entrepreneurs and artists have made expanding ownership and programming diversity in the television ecosystem"); LGBT Technology Partnership at 1 (describing "significant unintended consequences for minority and diverse programmers, especially those that focus on underserved communities such as the LGBT community"); Diverse Chambers of Commerce (USHCC, NGLCC, USPAAC, and USBC) ("This proposed rule represents a massive federal intervention into the television marketplace, which has never before been more dynamic or competitive. Far from serving the best interests of minority communities, this rule creates an unfair advantage for large tech companies at the expense of minority content creators and entrepreneurs."). Comments opposing the NPRM have been filed by: ASPIRA Association, Creators of Color, Cuban American National Council, Hispanic Leadership Fund, Hispanic Technology & Telecommunications Partnership, Independent Content Creators (representing VMe Media Inc., Manteca Media, Perfect Day Media, Hola! LA, Latin Heat Media, Freemind Beauty, Stateless Media, Feel Good TV, Freemind Ventures, Crossings TV), Japanese American Citizens League (joined by Asian Pacific American Public Affairs, Center for APA Women, Filipina Women's Network, National Federation of Filipino American Associations, Asian Pacific American Institute for Congressional Studies, National Asian Pacific American Women's Forum, Sikh American Legal Defense & Education Fund), LGBT Technology Partnership, MANA, A National Latina Organization, MMTC (joined by Asian Americans Advancing Justice, Asian Pacific American Institute For Congressional Studies, Latinos In Information Sciences And Technology Association, National Association Of Multicultural Digital Entrepreneurs, National Black Caucus of State Legislators, National Organization Of Black Elected Legislative Officials (NOBEL) Women, OCA – Asian Pacific American Advocates, Rainbow PUSH Coalition, National Puerto Rican Chamber Of Commerce), National Black Caucus of State Legislators, National Black Chamber of Commerce, National Hispanic Foundation of the Arts, National Puerto Rican Coalition, TechLatino: Latinos in Information Sciences and Technology Association, Tower of Babel, LLC (DBA Crossings TV), TV One LLC, United States Diverse Chambers (including United States Hispanic Chamber of Commerce, National Gay and Lesbian Chamber of Commerce, U.S. Pan Asian American Chamber of Commerce, U.S. Black Chamber), United States Hispanic Leadership Institute. ACT | The App Association also raises the concerns raised by the Congressional Black Caucus, noting that the Commission failed to and needs to consider the costs to and impacts on minority and independent programmers. Public Knowledge tries to deflect attention from this chorus of concerns by pointing to select statistics regarding the representation of minorities in MVPD programming and by the (comparably few) minority-owned programming interests that expressed support for the proposed rules. Public Knowledge Comments at 39-40. But as detailed herein at pages 28-29 and 48, the record evidence is clear that the proposal would harm independent and minority programming and provide no greater availability for online programming than is available today.

technology and platform providers and pirate box manufacturers to import the piracy problem into the pay-TV services environment for the first time, unrestricted and unprotected by licensing agreements or Commission rules."[65] The coalition concluded that given the uncertainties of whether standards bodies "can be developed to ensure the terms of contracts between programmers and MPVDs will be adhered to by non-contracting parties," the fact that "the voice of creatives in the process will be seriously diluted," "and the unrealistic two-year timeline for implementation, this is a process that is destined to fail."[66]

The Independent Content Creators, a group comprised of independent entertainment networks and production companies, explained that "[i]f this rule passes, Google will instead be able to strip-mine our creative work for free, while collecting valuable data on users' viewing history and monetizing it through ads. The Commission should not be in the business of placing its thumb on the scale by giving billions of dollars of business value to tech companies at the expense of independent programmers."[67]

A major coalition of music providers, who distribute through MVPDs over audio channels, also opposed the proposal. The Recording Industry Association of America, Inc., the National Music Publishers Association, the American Association of Independent Music, American Federation of Musicians, the Screen Actors Guild – American Federation of Television and Radio Artists, and SoundExchange, Inc., commented that the "Commission's proposal could create an unfair competitive landscape... The result would be to frustrate the

[65] CreativeFuture Comments at 8.

[66] *Id*. at 7.

[67] Independent Content Creators Comments at 6. "Independent Content Creators" refers to VME Media Inc., MNET America, Swirl Group, Condista Networks, Manteca Media, Perfect Day Media, Hola! LA, Latin Heat Media, TVOne, Unbelievable Entertainment, and Stateless Media.

incentives to create and disseminate copyrighted content via MVPD services and stifle innovation in business models that allow consumers access to music."[68]

A group of ten intellectual property scholars commented that the "zero-rate compulsory license [that would result from adoption of the NPRM] fundamentally disrupts copyright owners' ability to exercise control over their property" and that the "ability to choose whom to license their works to and on what terms is a key component of copyright owners' property interests."[69]

The grave threat to content creation posed by the NPRM is among the principal reasons that more than 150 members of Congress (including over half of the members of the House Democratic Caucus) have voiced their concerns to the Commission about its proposal. Congressional leaders have written to the Chairman that the proposed mandate "will jeopardize the incredible evolution of video distribution services,"[70] that "the proposal could lead to an expansion in the unauthorized distribution of copyrighted works,"[71] and that "contrary" to "suggestions that the content industry is supportive of the FCC's proposed rule," "there are substantial concerns on the part of the content industry, including television, film, and music, regarding the impact of the proposed rule on copyright protections, existing licensing agreements, and the rights of content creators."[72]

---

[68] Music Community Parties Comments at 4 (explaining that the proposed rules would "create an unfair competitive landscape by permitting some device and software developers to use music without abiding by the licensing conditions surrounding it, providing a windfall for third parties and undermining the protections for music owners that exist in the MVPD space today"). "Music Community Parties" refers to the Recording Industry Association of America, Inc., the National Music Publishers Association, the American Association of Independent Music, American Federation of Musicians, the Screen Actors Guild – American Federation of Television and Radio Artists, and SoundExchange, Inc.

[69] Intellectual Property Law Scholars Comments at 4.

[70] Letter from 60 Members of Congress, to Hon. Tom Wheeler, Chairman, FCC, MB Docket No. 16-42 (May 5, 2016).

[71] Letter from Rep. Bob Goodlatte, Chairman, and Rep. John Conyers, Ranking Member, Committee of the Judiciary, to Hon. Tom Wheeler, Chairman, FCC, MB Docket No. 16-42 (Apr. 29, 2016).

[72] Letter from Rep. Adam Schiff, Rep. Tony Cardenas, and Rep. Gene Green, U.S. Congress, to Hon. Tom Wheeler, Chairman, FCC, MB Docket No. 16-42 (Apr. 29, 2016).

The comments from the content community raised a number of more specific concerns as well, including the NPRM's dismantling of the business model of supporting content creation through advertising, and the ability of retail devices under the NPRM framework to ignore negotiated channel placement.

Advertising. MPAA wrote that the proposed rules "would also unfairly shift advertising revenues from those who invest in, and take considerable risks in, creating the programming, to third parties who seek to build their businesses on content they have not licensed."[73] The Association of National Advertisers, representing 700 companies with 10,000 brands that collectively spend over $250 billion in marketing and advertising annually, commented that the proposed rules "will have *great* potential to impact severely and adversely affect the advertising segment of our economy, e.g., by allowing for the potential use of ad overlays, insertion of additional material, degradation of existing content, and other unacceptable practices."[74] The ability to insert ads or overlays could change the fundamental nature of a programmer's mission; for example, C-SPAN states a "particular concern" that the NPRM could "undermine two of our fundamental operating characteristics: non-partisanship and non-commerciality," which would be "seriously compromised" if retail devices could "inappropriately associate our programs with either commercial products or political candidates or causes."[75]

Even those retail providers that do not engage in such obvious forms of interference with the original advertising will still disrupt the existing advertising business model that supports content creation. The Communications Workers of America (CWA) explain that lost ad revenues stemming from the proposal will have a negative impact on "the network, and the

[73] MPAA/SAG-AFTRA Comments at 7.

[74] Association of National Advertisers (ANA) Comments at 5 (emphasis in original).

[75] C-SPAN Comments at 1.

workers who create and produce content and who build, maintain, and service the network."[76] CWA encourages the Commission to "ensure that rules designed to promote competition in video navigation devices do not simply result in a shift of revenue and value from those who produce content and build the physical distribution network to innovators in re-packaging that content for targeted online advertising purposes."[77] ANA explains, "Advertisers would be in the position of not knowing who is responsible for the integrity of their ads, since the contractual relationships become substantially more uncertain under the NPRM's proposed regime in regard to MVPD content. It appears that advertisers would have to absorb significantly increased costs just in attempting to monitor where their ads appear, and whether they were the same messaging as they had originally put forth or not."[78] ANA's reply is illustrative of a recurring theme in this proceeding: the closer one looks at the practical impacts of the proposed rules, the more one discovers intractable problems for which the NPRM and its supporters offer no fix or remedy.

As explained in NCTA's comments, by undermining advertising, the proposed rules would hurt consumers by increasing the price MVPDs would have to pay for content, reducing the content that is available over MVPD systems, and potentially subjecting consumers to inappropriate advertising.[79]

Channel Placement. Another area of concern for the commenting content parties is channel placement.[80] TV One explains:

---

[76] CWA Comments at 5.

[77] *Id*. at 6.

[78] ANA Comments at 5.

[79] *See* NCTA Comments at 20, 48, 51-53, 55, 62, 79, 148-49; *see also* Steven S. Wildman, The Scary Economics of the NPRM's Navigation Device Rules, attached to NCTA Comments as Appendix C ("Economic White Paper") at 24-31, 35, 39; MPAA/SAG-AFTRA Comments at 7; ANA Comments at 4-10; Content Companies Comments at 7, 8, 12, 38.

[80] *See also* AT&T Comments at 37-40 (stating that the proposed rules "will undermine distribution agreements between MVPDs and programmers that often specify how a channel will be presented to consumers. If an MVPD is

> The loss of the negotiated right to particular placement – a very difficult right to secure for a diverse programmer – would cause particular harm to TV One and other minority programmers. Under the Proposal, a third party box manufacturer could place TV One anywhere on its interface, despite the fact that TV One's agreements with MVPDs often provide for specific tier or channel placement and result in TV One being grouped in a neighborhood with other channels serving the Black audience. These provisions are important to TV One's success because when the network is placed near other channels offering diverse content, it strengthens the likelihood that TV One will attract new viewers from a consumer that comes across TV One's programming via channel surfing. Without this ability – and combined with a potential loss of promotional opportunities – TV One's viewership, and thus its revenues, will shrink – threatening the continued vibrancy of diverse content.[81]

Public Knowledge tries to brush off concerns that retail devices could alter or ignore their negotiated channel placement, arguing that channel placement is "growing less important as a means of browsing and discovery.[82] But even Google has recognized that channels have not been displaced by search—which is why YouTube has channels on its front page. TV One explains how channel placement remains of vital importance to programmers, with channel placement clearly affecting exposure:

> The Commission states that it expects that [channel placement] provisions will be less important – and that the Proposal actually will benefit minority programming – because competitive interfaces, menus, and search functions will make it easier for consumers to find minority and special interest programming (including programming not carried by MVPDs), but this is simply not the case. First, niche and minority programming already have a difficult time securing a position that will result in higher exposure, and there is no reason to believe that, unbound by contractual requirements, a competitive interface will choose to make minority-owned and minority-targeted programming more prominent in guides or search results. Indeed, there is no reason to believe that these box manufacturers will even select any additional minority-themed programming for inclusion in their interface at all. Second, the third party box's search algorithm is likely to

---

unable to guarantee valuable channel placement to a programmer, then the programmer can be expected to seek higher total fees for its content – which will ultimately result in higher prices charged to consumers.").

[81] TV One Comments at 13-14. CVCC's comments state that Comcast has a 47.9% interest in TV One, but TV One bought out Comcast's stake in 2015. There should be no question about the independence of TV One's objections, considering that the same objections were raised by an overwhelming majority of other independent, minority-owned programmers and other supporters of diversity. *See supra* n.64 and accompanying text.

[82] Public Knowledge Comments at 46.

> prioritize content that viewers most often request—meaning that niche diverse content is likely to be buried, making it even harder for a viewer to come across and be exposed to TV One's programming or any other minority content, even if it is technically available on that platform.[83]

Public Knowledge also suggests that retail devices that alter channel placements could still "ensure" some measure of appropriate neighborhooding ("for example, that an adult-oriented program is not displayed while a device is in "Kids' Mode"); "a programmer need merely ensure that the metadata associated with such programming is complete and up to date."[84] But there is no "metadata" that defines or communicates channel position, prohibited proximities, brand protection requirements, and all of the other business requirements that MVPDs implement in order to comply with their license agreements.[85] While MVPD apps are designed to assure that their programming remains compliant with these requirements when displayed on retail devices through the app, there are no means in place to communicate these requirements on a disaggregated basis through information flows.[86] And even if such capability could be developed, nothing in the proposed rules requires retail devices to honor the channel placement and neighborhood terms of a programming agreement, or provides the enforcement tools to assure such compliance.

Public Knowledge claims that "nothing about the FCC's proposal will prevent programmers from contracting directly with device or platform vendors over rights and kinds of

---

[83] TV One Comments at 14-15.

[84] Public Knowledge Comments at 47.

[85] Sidney Skjei, A Technical Analysis of the FCC's Navigation Device Proposal at 22, attached to NCTA Comments as Appendix B ("Technical White Paper"). Verimatrix has warned against "creating overly complex formats to try to capture all future possible ways that content might be offered to a consumer." One central problem is that the standardization of metadata locks in existing business models, thereby raising "the potential of foreclosing an innovative offer that is elemental to a novel business model." Letter from Jim C. Williams, President and Founder, Media Strategies and Solutions, LLC, to Marlene H. Dortch, Secretary, FCC, MB Docket No. 16-42; CS Docket No. 97-80 (May 10, 2016) ("Verimatrix *Ex Parte*") at 2.

[86] Technical White Paper at 21.

access the FCC's proposal does not provide."[87] But what Public Knowledge is describing is *today's* world of direct licensing of content to online video providers – a world that the FCC is proposing to subvert with a zero-cost, unrestricted compulsory license. If new rules enable third parties to access, manipulate and monetize content however they choose, for free, why would they ever agree to pay for it and accept restrictions? If anything, since retail devices would have access to content for free regardless of licensing agreements, the negotiation dynamics would be completely changed. Popular device platforms might instead ask programmers to pay them in order to secure preferred channel placement or priority search results, with those programmers who are unable or unwilling to pay relegated to the least desirable placement, if any, on the retail platform.[88] It is no wonder that so many content owners have risen in strong opposition to having their content commandeered by parties that have not even paid for it.

B. The NPRM Proponents Minimize and Distort Content Owners' Serious Copyright Concerns

Members of the CVCC have tried to obfuscate and minimize the serious copyright protection concerns raised in this proceeding by lumping all of them under the characterization of piracy. In a recent *ex parte*, they dismiss the concerns of content owners as an "irrelevant" "attempt at misdirection," claiming that there is the potential for piracy with any device that

[87] Public Knowledge Comments at 45.

[88] Google currently provides priority placement to paid advertisements placed at the very top of search results. Apple monetizes by imposing the so-called "Apple tax" of 30% of app revenue, forcing some providers to flow those surcharges through to consumers or to prohibit transactions from occurring within the app. *See* Amanda Schupak, *New YouTube Subscription Will Cost More to Buy on Apple Devices*, CBS NEWS (Oct. 22, 2015), http://www.cbsnews.com/news/new-youtube-subscription-will-cost-more-on-apple-devices/ ("When YouTube's Red subscription streaming service launches Oct. 28, you'll be able to pay $9.99 for a month's worth of videos uninterrupted by advertisements. Unless you're on a iPhone, in which case, you'll have to pony up $12.99. … Apple takes a 30 percent cut of revenues for subscriptions sold via in-app purchases. And Google, which owns YouTube, will pass that extra cost onto subscribers."); Vudu, *The New Vudu Player for iPhone and iPad*, VUDU.COM (Dec. 23, 2014), http://blog.vudu.com/?p=11313 ("FAQs - Why can't I purchase or rent through the app? While we would love to make owning or renting through the VUDU Player app [sic], Apple's fees for in-app purchases makes it economically unfeasible to do so. You can, however, still browse and shop VUDU using your mobile device's web browser.").

connects to the Internet, and that "[i]t is hard to see how giving consumers greater access to lawful content would increase their appetite for unlawful content."[89] It is this glib contention that is the misdirection. While NCTA and others have demonstrated that the FCC's proposal would indeed facilitate piracy by elevating such unauthorized channels onto a level playing field with legitimate content and bringing all of the piracy of the Internet into the television, that is not the primary content issue in this case.[90] The larger issue for many parties is the fact that the NPRM's disaggregation proposal would enable retail devices to alter and manipulate content licensed to the MVPDs and incorporate that content into their own, different, unlicensed and monetized services without the permission of the content owner, without paying them, and without complying with the content owner's terms. It should be hard *not* to see why content owners do not want the FCC to champion and sanction the serial misappropriation of all of the content they license to MVPDs.

C. Programming Cannot Adequately Be Protected by Litigation

The NPRM's proponents fail to materially address any of the concerns that the NPRM proposal would contribute to misappropriation and manipulation of content and piracy. Public Knowledge claims that "[d]evices that are not compliant [in terms of protecting content] will have no access to MVPD programming, and devices that become non-compliant risk having their access to MVPD programming revoked."[91] In the first place, nothing in the NPRM indicates that MVPDs would be permitted to deny access to devices on the grounds of copyright infringement. Moreover, even if such unilateral action would be allowed, Public Knowledge does not offer any comprehensive commercially and technically workable demonstration of how an MVPD could

[89] Letter from Kate Forscey, Associate Counsel for Government Affairs, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, MB Docket No. 16-42 (May 9, 2016) ("Public Knowledge May 9, 2016 *Ex Parte*").

[90] *See* NCTA Comments at 100-106.

[91] Public Knowledge Comments at 51.

do it. Instead, the proponents of the mandate would remove modern technological protection measures, agreements, audits, and any other enforcement tools and relegate content owners to prosecuting copyright infringement in court.[92]

Reliance on litigation as the primary means of protecting content would lead to catastrophic market failure. As MPAA explains, "content owners do not make primary use of litigation in the marketplace in order to enforce and protect their rights. The primary mechanism for copyright holders to enforce their exclusive rights is program license agreements. It is misplaced to assume that enforcement via litigation could compensate for the displacement of detailed arrangements that have been carefully negotiated between programmers and distributors."[93]

For example, broadcast networks segment their markets with affiliation agreements that define the permissible DMA and myriad other terms. They do not release their content and leave it to copyright infringement litigation to determine the permissible terms for affiliate use. Likewise, program producers that license content to networks will segment the permissible downstream markets by license, and the networks that include that program will window, segment, and define the economic terms for distribution among various distributors through license. It is not left to infringement litigation to determine what is acceptable for the network or distributor to do with copyrighted content.

In MVPD distribution, those licensing decisions are protected with technological protection measures protected under the DMCA. Just last fall, the U.S. Copyright Office

---

[92] *See* Public Knowledge Comments at 51 ("In candor, Public Knowledge believes that universal principles of copyright law such as secondary liability are enough to ensure that the legitimate interests of copyright owners are protected…."). *See also* MPAA/SAG-AFTRA Comments at 17 ("Some argue the proposal does not interfere with copyright holders' exclusive rights because copyright holders would remain free to sue third parties that use their content in ways that infringe their rights.").

[93] MPAA/SAG-AFTRA Comments at 17.

rejected Public Knowledge's requests to override such technological protection measures, finding that there is no blanket claim to fair use of programming or networks, and there are ample avenues for access to programming from a variety of licensed sources.[94]

ANA agrees that litigation is no substitute for technological protection measures: "It is small comfort that advertisers might potentially be able to enforce their rights in court, presuming they could track their ads, identify whom they could sue, and the like, as this litigation would be very expensive, highly uncertain, and enormously time-consuming."[95] The Content Companies similarly explained:

> The Notice's assertion that copyright law currently serves – and can effectively serve in the new marketplace – as the sole method of protecting programmers' rights is also misplaced. Copyright litigation is lengthy and resource-intensive for all parties, and limiting programmers to that remedy alone would supplant exclusive rights defined in licensing agreements, including the right to enforce those rights via contract law. Indeed, many contractual provisions designed to secure programmers' content are not covered by copyright. The serial trips to court mandated by copyright litigation would be even more difficult for smaller programmers with fewer resources, for whom lawsuits may not be a realistic option. And all programmers would confront an environment in which they are forced to play "whack-a-mole" – repeatedly having to fight to undo damaging violations after the fact each and every time a third party attempts to commercialize content (perhaps in the guise of 'innovation') by ignoring programmers' rights. In short, the potential remedy of copyright litigation does not begin to approximate the essential controls and protections that can be secured through licensing between parties in privity, and so has always been considered a last resort not a first line of defense, against infringement. Ignoring this reality would be irrational.[96]

The Commission's proposal circumvents these technological protection measures and turns the clock back to "whack-a-mole" infringement litigation. As MPAA and SAG-AFTRA

---

[94] U.S. Copyright Office, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 80 Fed. Reg. 65944, 65960 (Oct. 28, 2015).

[95] ANA Comments at 5.

[96] Content Companies Comments at 31.

explained, "Programmers may not even be able to find these third parties, especially if they are a foreign device manufacturer, or an application developer somewhere out on the vast Internet."[97]

The Commission cannot lawfully or responsibly leave content owners without an effective means to protect themselves from potential massive copyright infringement that would be made possible by the Commission's own regulations.

D. Programming Cannot Adequately be Protected by Additional Conditions

NAB similarly protests the potential infringement of its members' programming licenses but suggests that the Commission can cure the problem by adopting conditions to protect all terms of retransmission consent agreements, including terms for advertising and promotional material, channel position, and embedded advertising, and by adopting a licensing and certification program to effectuate compliance.[98] NCTA agrees with NAB that it is essential that the terms of retransmission consent agreements (like all programming agreements) be honored by retail devices. A retransmission consent agreement might assign a broadcast signal to a particular channel, in a defined neighborhood, with embedded advertising, and agreed upon promotional arrangements, and define the permissible distribution and the security to ensure it. The FCC should not be opening the gate for third parties to ignore those terms, change the channel, realign the neighborhood, sell the audience for overlaid ads, and defy distribution limits and security requirements.

But the FCC would not be able to close those floodgates and protect the terms of programming licenses and agreements by simply saying so explicitly in an amended rule. Saying that license terms must be honored would not make it so. As NCTA demonstrated in its

[97] MPAA/SAG-AFTRA Comments at 18. The Director's Guild further noted the difficulty in removing pirated content from the Internet. Director's Guild/IATSE Comments at 6.

[98] NAB Comments at 3.

Comments, neither DRM systems nor conditional access systems can be relied upon to ensure protection of these license terms.[99] Today, MVPDs can ensure that license terms are honored when content is presented through retail devices such as a Roku or an iPad by using the MVPD app and an enforceable trust infrastructure. But the proposed rules would strip both of these from the equation for retail devices that access MVPD content through the disaggregated information flows. Without these built-in protections, even if the FCC now modifies its rules to declare that retail devices must honor licensing agreement terms, or certain enumerated standard terms such as for channel placement or advertising, such requirements would be hollow because there would be no tools to practically or legally enforce them against device manufacturers and third-party app developers over which the FCC has disclaimed enforcement jurisdiction.

CVCC offers the same illusory hope that advertising terms can be protected with the addition of words. Just days after one CVCC member dismissed concerns that third-party device creators would or could disrupt advertising within pay-TV programming as "unfounded,"[100] CVCC invited an amended rule that would limit a third party from replacing or obscuring the advertising contained in MVPD programming.[101] But the suggested protection is far narrower than the advertising requirements in program license agreements: it leaves open the opportunity for third parties to monetize programming for which they have no license and no financial

[99] *See, e.g.*, NCTA Comments at 78 ("[U]nder the FCC's proposal, the MVPD would be unable to run software controls within a trusted execution environment within the third-party device or app … [a]nd because an MVPD would have no license or other business-to-business agreement with the device manufacturer or app developer, an MVPD would have no power to audit a device, app, its provider or affiliates, or require response to inquiries investigating compliance"); 92 ("the FCC proposes to remove and entirely circumvent the MVPDs' technological protection measures … it fails to provide any tools that MVPDs might rely upon to ensure that channel location is respected. The DRM cannot secure channel location when decoupled from the guide or app. The NPRM would prohibit MVPDs from running code within the third-party device or app. The NPRM would bar business relationships between MVPDs and third-parties that could enforce channel-placement requirements through contract. Nor is there any technical or practical means to monitor or enforce third-party compliance.").

[100] Public Knowledge May 9, 2016 *Ex Parte*.

[101] *See* 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).

responsibilities with ads around the content, within search results, without regard to brand exclusivity arrangements, and in any other way with "consumer volition." And even those narrow limitations are chimerical, because the NPRM proposes no technical, contractual, or legal tools to enforce them against device manufacturers and third-party app developers over which the FCC has disclaimed enforcement jurisdiction.

The addition of mere words to suggest copyright protections are, as NCTA explained in its Comments, comparable to the "FBI Warning" from analog VCR days – conveying an unenforceable message to please be on good behavior while handling the highest value digital video content carried by all MVPDs.[102] Lip service to protecting copyright and advertising, recourse to copyright infringement suits, and unenforceable certifications cannot replace the licensing and certification of the trust infrastructure that secures retransmission consent and all programming licenses today.

The only way to "fix" the NPRM is to abandon the premise that MVPD service can be unbundled from apps, license agreements, and the trust infrastructure, and instead build from the apps-based solutions that the market has developed. The FCC's disaggregation approach is not fixable because it offers no privity between content owners and retail device providers and no means for MVPDs to enforce any rules or certifications.

E. Imposition of a Compulsory License Would Be Unwarranted and Unlawful

Numerous content owners liken the impact of the NPRM's proposal to a new compulsory license that effectively requires any content owner licensing its content to any one MVPD to be subjected to taking of that content by any third party device or app provider that connects to that

[102] *See* NCTA Comments at 93.

MVPD's unbundled "information flows."[103] The Consumer Federation of America's economic analysis seeks to justify this result by noting with approval the compulsory license imposed on broadcasters by Congress in the Copyright Act of 1976. CFA states that "it had become clear that cable could not succeed as a competitor to over-the-air broadcasting without access to the 'marque' content that the broadcasters controlled."[104] But this comparison fails for several reasons.

First, as MPAA notes, "Only Congress may create compulsory licenses, which operate as statutory exceptions to copyright holders' rights under the Copyright Act,"[105] and the Content Companies explain that "Congress has historically provided for compulsory licenses only in rare circumstances through specific statutory grants."[106] Thus, as the Content Companies explained, the FCC has no authority to create a new compulsory license.

Second, MPAA documents that compulsory licenses created by Congress are "carefully calibrated, provide for royalty payments to compensate copyright owners, and prohibit alterations of the programming or advertisements."[107] Even Congress would exceed its constitutional bounds if it enacted the type of compulsory license proposed by the NPRM that

[103] *See, e.g.*, MPAA/SAG-AFTRA Comments at 8-9; Content Companies Comments at 39-40; Comcast Comments at 48, 74, 75.

[104] Mark Cooper, Cable Market Power – The Never Ending Story of Consumer Overcharges and Excess Corporate Profits in Video and Broadband at 2 ("Cooper Study").

[105] MPAA/SAG-AFTRA Comments at 8.

[106] Content Companies Comments at 39. The Content Companies also note that "Congress gave no hint of any desire to permit the Commission to use Section 629 as a vehicle for creating a compulsory copyright license for navigation device manufacturers or services." *Id.*

[107] MPAA/SAG-AFTRA Comments at 8. *See also* Content Companies Comments at 39 ("In those limited instances where Congress has created statutory licenses to serve as an exception to copyright owners' exclusive rights, it has said so in clear and explicit terms, and has historically included language restricting content manipulation and mandating compensation payments to content owners.").

provides no restriction on that device's manipulation, alternation or redistribution of the content and no compensation to be paid.[108]

Third, there is no basis for such FCC intervention in the marketplace given the ability of OVDs to license content from programmers. The Comments filed by the Center for Individual Freedom cite a recent survey that reported that 98% of premium films and 94% of premium television series were digitally available from at least one licensed online provider.[109] Netflix and Amazon each have more U.S. OVD subscribers than any MVPD in the country, and each has enormous libraries of content.[110] This market is very different from the market considered by Congress when it created the broadcast compulsory license.[111] The U.S. Copyright Office (which unlike the FCC is the expert agency charged with administering the Copyright Act) has opposed the creation of new compulsory licenses, and has stated that it views "statutory licenses as a mechanism of last resort that must be narrowly tailored to address a specific failure in a specifically defined market."[112] No such "last resort" is needed in a market in which valuable

---

[108] *See* Content Companies Comments at 42 ("[T]he Commission's proposals effectively create a compulsory license. That would violate the Takings Clause, since the proposed rules seize content owners' intellectual property without just compensation. Even if the Commission's proposed rules are not viewed as a compulsory license, they take content owners' intellectual property and give it to navigation device companies for their own profit and revenue exploitation. The Constitution prohibits this taking of intellectual property, just as it would prohibit the taking of physical property.").

[109] Center for Individual Freedom (CFIF) Comments at 2 (citing SNL Kagan, U.S. Availability of Film and TV Titles in the Digital Age (March 2016), http://go.snl.com/rs/080-PQS 123/images/U.S.%20Availability%20of%20Film%20and%20TV%20Titles%20in%20the%20Digital%20Age.pdf)).

[110] *See* Chris Isidore, *Amazon Prime Now Reaches Nearly Half of U.S. Households*, CNN MONEY (Jan. 26, 2016), http://money.cnn.com/2016/01/26/technology/amazon-prime-memberships/index.html (discussing report by analyst that estimates that approximately 54 million U.S. households have an Amazon Prime membership); Jeff Baumgartner, *Netflix Eclipses 75M Subs Worldwide*, MULTICHANNEL NEWS (Jan. 19, 2016), available at http://www.multichannel.com/news/content/netflix-eclipses-75m-subs-worldwide/396659 (noting that Netflix expanded its total number of U.S. subscribers to 44.74 million in the fourth quarter of 2015).

[111] Cooper Study at 2.

[112] MPAA/SAG-AFTRA Comments at 9 (quoting U.S. Copyright Office, *Notice of Inquiry re Orphan Works and Mass Digitization*, 77 Fed. Reg. 64559 (Oct. 12, 2012)).

content is available pervasively to competing video platforms that are willing to negotiate copyright licensing terms.

F. The NPRM Proponents Do Not Even Address Protection of MVPDs' or Guide Providers' Copyright Interests

While the NPRM's supporters at least profess that they would try to protect the copyright interests of programmers, they do not even address, let alone protect against, the infringement of the MVPDs' copyright in the "collective works" and "compilations" of programming and additional content that comprise the service that MVPDs offer consumers, which would result when retail devices and apps alter and repackage MVPDs' services as their own.[113] They explicitly assert their intent to change the presentation of the service, and the NPRM offers no controls to prevent this; indeed, it encourages such a result.

Likewise, the NPRM and its supporters simply assume, without justification, that program guide data and one supplier's program identification system may be extracted from guides and conveyed to unlicensed third parties. As the Commission has known for at least a decade, as was explained in DSTAC, and as confirmed by Gracenote, MVPDs license copyrighted guide data for limited uses from third parties and exercise creative judgment in compiling the inputs into unique programming guides and user interfaces that distinguish their services from those of competitors. In so doing, MVPDs enjoy their own intellectual property protections.[114] Even CableCARD-enabled retail devices do not receive the information that the

[113] *See* NCTA Comments at 58 (citing Copyright Act provisions and supporting case law).

[114] *See* Letter from Stephen H. Kay, Executive Vice President & General Counsel, Gemstar-TV Guide, to Marlene H. Dortch, Secretary, FCC, CS Docket No. 97-80, MB Docket No. 00-67 (Nov. 14, 2007); DSTAC Final Report at 295 (DSTAC WG4 at 160); Theodore B. Olson, Helgi C. Walker, and Jack N. Goodman, The FCC's "Competitive Navigation" Mandate: A Legal Analysis of Statutory and Constitutional Limits on FCC Authority, Attached to NCTA Comments as Appendix A, at 53 ("Legal White Paper").

NPRM proposes be released to third-parties.[115] As Gracenote explains, Gracenote competes with Rovi, Ericsson, and others in a robust market. Programming metadata, including proprietary ID numbers, is not factual non-copyrightable material free for extraction, but protected intellectual property that it is willing to offer at reasonable and nondiscriminatory prices to anyone who wishes to purchase them, but that the Commission is not free to give away.[116] In addition, guides themselves are subject to complex intellectual property rights, with a record of patent litigation and large law suits.[117]

The proposed rules simply call for MVPDs to disregard their contracts, infringe intellectual property and copyright, and even post the data without securing it – undermining the very economics for the TV metadata industry to collect and provide this content in the first place.

TiVo is not so cavalier about intellectual property rights when its own intellectual property is concerned. Ignoring the right of copyright owners to license devices, platforms and distributors is like saying TiVo's patents, once granted for use by an MVPD, can be used by any third party device manufacturer that connects to the MVPD.

---

[115] TiVo licenses data from third parties at its own expense for its guide. OCUR manufacturers like Hauppauge rely on Microsoft to do the same.

[116] Gracenote also explains that EIDR – the programming code that the NPRM suggests all MVPDs should transmit with one information flow – is not a standard program identifier nor does it cover all programming. Instead, it is just one among competing sources. *See* Gracenote Comments at 7-8.

[117] *See Gemstar-TV Guide, Scientific-Atlanta Settle Patent Lawsuits,* SOCALTECH (June 2, 2005), http://www.socaltech.com/gemstar_tv_guide_scientific_atlanta_settle_patent_lawsuits/s-0002006.html ("The companies estimated that license payments from Scientific-Atlanta to Gemstar-TV Guide would be worth $154M, and payments from Gemstar-TV Guide to Scientific-Atlanta $89M."); *Gemstar-TV Guide In Deal With Verizon*, SOCALTECH (May 2, 2007), http://www.socaltech.com/gemstar_tv_guide_in_deal_with_verison/s-0008892.html; *Gemstar, Yahoo In Licensing Deal*, SOCALTECH (Sept. 15, 2006), http://www.socaltech.com/gemstar_yahoo_in_licensing_deal/s-0005346.html; *Gemstar Grants Patent License To Pioneer*, SOCALTECH (Aug. 30, 2005), http:/www.socaltech.com/gemstar_grants_patent _license_to_pioneer/s0002317.html; *Gemstar-TV Guide, LG Electronics in Licensing Deal,* SOCALTECH (Jan. 8, 2004), http://www.socaltech.com/gemstar_tv_guide_lg_electronics_in_licensing_deal/s-0000025.html; *Gemstar-TV Guide Extends Mitsubishi License*, SOCALTECH (July 18, 2007), http:///www.socaltech.com/gemstar_tv_guide_ extends_mitsubishi_license/s-0010175.html; *Gemstar Expands License With Sony*, SOCALTECH (Mar. 24, 2005), http://www.socaltech.com/gemstar_expands_license_with_sony/s-0001721.html; *Gemstar Signs Samsung*, SOCALTECH (May 2, 2006), http://www.socaltech.com/gemstar_signs_samsung/s-0003882.html ("Gemstar holds patents covering its VCR Plus system for setting up VCR recording times, along with patents around interactive programming guides, and has licensed that technology to a large number of electronics manufacturers.").

The NPRM is clearly not fulfilling the Chairman's commitment that "[e]xisting content distribution deals, licensing terms, and conditions will remain unchanged," and that "the Commission will not interfere with the business relationships … between MVPDs and their customers."[118] The market knows what protecting copyright looks like: Netflix no longer makes APIs available for third parties to ingest its content into their own platforms to present Netflix content through the third party's interface, preferring instead to control the presentation through its app on all third party devices.[119] And in DSTAC, Amazon emphatically rejected the notion of opening up the trusted environment it uses in Kindle to any third party.[120] The only way to protect intellectual property is to drop the proposed unbundling mandate.

III. THE PROPONENTS FAILED TO DEMONSTRATE THAT THE PROPOSED MANDATE IS THE BEST WAY TO PROMOTE CONSUMER CHOICE FOR DEVICES OR CONTENT

One of the most critical failures of the NPRM and the comments supporting it is their failure to articulate a compelling, sound explanation for why the proposed costly set-top box mandate would be the best path forward in the first place.

A. The Promised Benefits of the Proposed Mandate Are Illusory

The fact that most MVPD customers lease at least one device from their MVPD does not mean, as CVCC claims, that they are "denied the opportunity to choose which device best suits

[118] *FCC Chairman Proposal to Unlock the Set-Top-Box: Creating Choice & Innovation* (Jan. 27, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0127/DOC-337449A1.pdf ("Chairman's Fact Sheet").

[119] *See* NCTA Comments at 63-65.

[120] *See* Transcript of Jul. 7, 2015 DSTAC meeting at 37-38 (Mr. Chaboud [from Amazon]: "when we make a device the code that runs in the trusted execution environment on that device is our code or code from the SOC vendor and that's it, right. And the reason we do that is because we put very critical keys for DRM in that context that would be accessible by any code running in that context. So if we were to run code from a third party they would have access to our entire sort of critical DRM and provisioning keys and it would compromise our security. So that won't happen."). *See also id*. at 41 (Mr. Chaboud: "I want to make the point clear that there is no requirement that code be downloaded and executed in our trusted execution environments.").

their needs."[121] On the contrary, nearly two-thirds of U.S. TV homes now have at least one TV connected to the Internet via a Roku, Apple TV, Amazon Fire TV, or other streaming device, and a new study released in April 2016 found that there are now more connected TV devices in the United States than MVPD set-top boxes.[122] MVPD customers can now also use more of such retail devices, tablets and smartphones to watch MVPD programming than there are operator-supplied set-top boxes. In addition, consumers may access individual programmer apps on an authenticated or individual subscription basis.[123] Renting a set-top box from an MVPD has not denied consumers the ability to use these increasingly ubiquitous streaming devices[124] any more so than those devices have denied consumers the ability to use an MVPD's set-top box.

The proponents next suggest that even if consumers are not prevented from buying other devices at retail, the proposed rule would save consumers money by relieving them of spending a supposed $231 per year renting set-top boxes, a cost that they claim has soared by 185% since 1994.[125] NCTA has already demonstrated that the real cost of renting functionally-equivalent devices has declined.[126] Moreover, the TiVo device, the poster child for third party retail devices, has typically cost more than renting a cable DVR.[127] Rather than saving consumers on set-top box costs, the proposed rules would raise consumer costs[128] and just change who they

---

[121] CVCC Comments at 14.

[122] NCTA Comments at 12 (citing Jeff Baumgartner, *Study: Connected TV Devices Eclipse Pay TV Set-Tops*, MULTICHANNEL NEWS (Apr. 22, 2016), http://www.multichannel.com/news/distribution/study-connected-tv-devices-eclipse-pay-tv-set-tops/404377).

[123] *See* Appendix B, Selection of Programmer Apps.

[124] David Katzmaier, *Roku vs. Apple TV vs. Chromecast vs. Amazon Fire TV vs. Android TV: Which Streamer Should You Buy?*, CNET (Apr. 20, 2016), http://www.cnet.com/news/chromecast-vs-apple-tv-vs-roku-3-which-media-streamer-should-you-buy.

[125] TiVo Comments at 9.

[126] NCTA Comments at 138-139 and n.329; Economic White Paper at 17-19.

[127] NCTA Comments at 140.

[128] As detailed in NCTA Comments, the proposed rules would not help consumers cut the cord or lower costs: a cable subscription would still be required, and prices would go up as *all* subscribers bear the massive costs to invent

pay. If consumers are really to save the money they now spend on set-top boxes, the answer is to eliminate the box, not "unlock" it. All of the ten largest MVPDs now support "boxless" viewing of their content on customer-owned tablets, Smart TVs and other devices, but the FCC's proposed parity rules would put an end to those programs,[129] and also effectively require a new second intermediary box in the home (rented from their MVPD) of every consumer using a retail box that relies upon the information flows.[130] The proposed rules would stifle rather than "accelerate" boxless delivery via apps, as CFA claims.[131] And for that reason, among many others, rather than save anyone money, the FCC's proposed mandate would "lock in the box" costs for consumers – which would be just fine with TiVo, which hopes to be able to keep selling its set-top boxes for years to come to the cable operators who make up the overwhelming bulk of its customers, rather than see the box reduced to a downloadable app.

The proponents also contend that the new mandate would spare consumers of the "cumbersome situation" of navigating between multiple MVPD and OVD devices using multiple remotes.[132] But any consumer can use a universal remote that is capable of controlling both MVPD and third-party devices;[133] new offerings such as the new Samsung smart remotes (that automatically detect the HDMI port associated with each connected consumer device to enable

---

new standards, clear new intellectual property rights, and develop, test and deploy new equipment, and support the ongoing leasing and electricity costs of a second box in the home just to serve the retail box. *See* NCTA Comments at 18-20. *See also* NRDC Comments at 1-2 (discussing potential increases in consumers' energy bills).

[129] NCTA Comments at 134-135. The proposed parity rules would lead to a move away from boxless solutions because they require an MVPD that provides boxless access to its content *via app* to any one device to also provide boxless access to content to all third-party apps or devices *without an app*. As NCTA previously noted, this would be "a nearly impossible hurdle," and would chill further app development efforts.

[130] NCTA Comments at 130-132. Satellite and IPTV providers will need to utilize a second box, while the functional requirements of the proposal will require an additional box to serve the "information flows" properly to third-party devices or apps for other MVPDs.

[131] CFA Comments at 10.

[132] Information Technology Industry Council Comments at 5-6. Google and Amazon are members of ITIC.

[133] NCTA Comments at 15-16 (citing as example Logitech, Harmony Remotes, http://www.logitech.com/en-us/universal-remotes (last visited Apr. 19, 2016)).

seamless switching between different sources using a single remote without even having to press the "input" button to switch HDMI ports); and technologies such as HDMI CEC (a control function that lets an A/V component control another if they are connected via HDMI cables) to eliminate the hassle of having multiple remote controls.[134]

Even if the proposed rules aren't needed to allow consumers to buy retail devices to access their MVPD programming, or to save consumers money, or enable them to access all of their content with a single remote, the proponents contend the proposed mandate is needed to make OVD content more accessible to consumers. They claim that "monopoly" MVPD set-top boxes "restrict consumers' ability to stream new Internet programming, thus suppressing an entire industry of new content creators."[135] Their purported theory is that if only the FCC would enable third party devices to combine MVPD and OVD content together in a single device, "consumers would enjoy even greater opportunities to discover independent and diverse content, as offerings that have never before graced television screens suddenly become accessible through competitive navigation devices."[136] This central argument to the proponents' case is deeply flawed, for several reasons:

MVPD set-top boxes clearly are not preventing consumers from accessing OVD content. Netflix and Amazon each have more paid video subscribers in the United States than any MVPD.[137] Netflix alone reported that its subscribers watched 42.5 billion hours of streaming

---

[134] *Id*. at 16.

[135] CVCC Comments at 8.

[136] *Id*. at 6.

[137] *See* Jeff Baumgartner, *Netflix Eclipses 75M Subs Worldwide*, MULTICHANNEL NEWS (Jan. 19, 2016), available at http://www.multichannel.com/news/content/netflix-eclipses-75m-subs-worldwide/396659 (noting that Netflix expanded its total number of U.S. subscribers to 44.74 million in the fourth quarter of 2015); Chris Isidore, *Amazon Prime Now Reaches Nearly Half of U.S. Households*, CNN MONEY (Jan. 26, 2016), http://money.cnn.com/2016/01/26/technology/amazon-prime-memberships/index.html (discussing report by analyst that estimates that approximately 54 million U.S. households have an Amazon Prime membership).

video in 2015,[138] and millennials age 18-34 now watch more than half of their TV through streaming.[139]

Online distribution has already revolutionized the ability of even the smallest independent producer or programmer to successfully disseminate their content to millions of consumers. Content creators and owners have more options than ever for reaching consumers, with or without any particular MVPD's support. Roku supports 3,400 channels, and it explains that "Roku's open platform and easy-to-use development tools have allowed niche programming to flourish and enabled local communities, local institutions and other independent content producers to create their own Roku channels."[140] Anyone that can build an app can deliver video to consumers through app stores available on millions of retail devices, including Smart TVs.[141] Amazon just announced the launch of a new Amazon Video Direct service that enables creators to upload videos to Amazon that will be viewable by all Amazon customers via an ad-supported model, alongside studio-created TV shows and movies.[142] The top five YouTube stars have twice as many subscribers as all U.S. MVPDs combined, and many YouTube success stories

---

[138] Netflix, Quarterly Investor Letter from Reed Hastings, CEO, and David Wells, CFO, Netflix, to Netflix Shareholders (Jan. 19, 2016) at 5, available at http://files.shareholder.com/downloads/NFLX/1371814617x0x870685/C6213FF9-5498-4084-A0FF-74363CEE35A1/Q4_15_Letter_to_Shareholders_-_COMBINED.pdf.

[139] Press Release, Horowitz Research, Millennials Stream More than Half of their TV; More Likely to Turn to Netflix for TV than Live, Says Horowitz (May 4, 2016), available at http://www.horowitzresearch.com/news/press-releases/millennials-stream-more-than-half-of-their-tv-more-likely-to-turn-to-netflix-for-tv-than-live-says-horowitz/.

[140] Roku Comments at 4.

[141] *See, e.g.*, Opera TV Store – Apps Made for TV, Opera Business (last visited May 19, 2016), http://www.operasoftware.com/products/tv/tv-store ("The Opera TV Store is an HTML5-based storefront of exciting web apps optimized for TV. Opera TV Store apps run from the cloud and suit any screen size or resolution.").

[142] *See* Ron Amadeo, *"Amazon Video Direct" Takes Aim at the Professional Side of YouTube*, ARS TECHNICA (May 10, 2016), http://arstechnica.com/business/2016/05/amazon-video-direct-takes-aim-at-the-professional-side-of-youtube/.

have led to deals with television and movie studios.[143] And seemingly every day, new online video offerings are announced or previewed – by BitTorrent and Samsung in just the past week.[144] No MVPD can act as a gatekeeper that can deny a content producer ubiquitous access to consumers.

Consumers can already watch OVD content on numerous devices, including many that also display content from MVPDs.[145] MVPD set-top boxes are not assured of being the dominant, primary device in the home because of exclusive access to most of the most-desired content. The Center for Individual Freedom comments report that 98% of premium films and 94% of premium television series were digitally available from a non-MVPD online service.[146] Even live sports are increasingly available from multiple options, including content directly available from apps offered by professional leagues, and ESPN is available on Roku and Sling TV.[147] Last month, the NFL entered into a new streaming deal with Twitter for Thursday Night

---

[143] *See* Cecilia Kang, *The Real Reasons Why YouTube's 5 Biggest Stars Became Millionaires*, WASHINGTON POST (Jul. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/07/23/how-these-5-youtube-stars-became-millionaires-and-why-you-wont-be-joining-them-anytime-soon/.

[144] *See* Gerry Smith and Lucas Shaw, *Samsung Explores Online TV Service with Cable Networks*, BLOOMBERG TECHNOLOGY (May 19, 2016), http://www.bloomberg.com/news/articles/2016-05-19/samsung-said-to-explore-online-tv-service-with-cable-networks; Matthew Ingram, *BitTorrent's New Streaming TV Service Has 1 Unique Feature, But Will It Be Enough?*, FORTUNE (May 18, 2016), http://fortune.com/2016/05/18/bittorrent-streaming-tv/.

[145] *See* NCTA Comments at 14-15.

[146] CFIF Comments at 2. *See also* MPAA/SAG-AFTRA Comments at 2 ("American audiences today can choose among more than 115 online services to legally access television and film content over the Internet, up from essentially zero in 1997. Viewers used these services to access 66.3 billion television episodes and 7.1 billion movies in 2014, up 229 percent and 1,132 percent, respectively, from 2009.").

[147] *See, e.g.*, MLB.TV, http://mlb.mlb.com/mlb/subscriptions/index.jsp?c_id=mlb&affiliateId=mlbMENU (last visited May 20, 2016); NHL.TV, https://subscribe.nhl.com/ (last visited May 20, 2016); Roku Channel Store, WatchESPN Channel, https://channelstore.roku.com/details/34376/watchespn (last visited May 20, 2016); Sling TV, Best of Live TV Service, https://www.sling.com/service (last visited May 20, 2016) (listing ESPN and ESPN2 among channels included in Best of Live TV service for $20/month).

Football.[148] As Roku stated in its comments, "[t]he cable company is one option for accessing TV content, but, increasingly, it is not the only option."[149]

With online distribution still in its relative infancy and growing exponentially, these trends will only intensify. The FCC's help is not needed to assure that MVPD set-top boxes cannot get in the way of consumer access to online content from the widest possible variety of sources on a wide variety of devices. Millions of consumers are already viewing video programming from multiple (MVPD and OVD) sources, and so all video providers have an incentive to make their services as available as possible in whatever manner their paying customers desire.

NCTA agrees with sixty members of Congress, who recently wrote to the Commission that "it is unclear what purpose the new rules would serve in this era of unprecedented consumer choice."[150] Similarly, CALinnovates commented that, "The market is functioning well, with rich offerings and mixes of content and technologies vying for eyeballs across platforms, devices and generations. To repeat: Why an agency would step in at this moment to damn a rushing river is curious, if not misguided. That is why CALinnovates – a coalition of technology leaders, startups, and entrepreneurs – opposes the Commission's plan to interject itself into this thriving, vibrant market with a one-size-fits-all set-top box mandate that will stifle innovation."[151]

NCTA also agrees with the League of United Latin American Citizens (LULAC) that it is "hard to understand why the Commission is under the impression that blending over-the-top programming with paid-TV channels in a 3rd party interface will lead to more revenue for

---

[148] *See* Press Release, National Football League, National Football League and Twitter Announce Streaming Partnership for Thursday Night Football (Apr. 5, 2016), available at https://nflcommunications.com/Pages/National-Football-League-and-Twitter-Announce-Streaming-Partnership-for-Thursday-Night-Football.aspx.

[149] Roku Comments at 2.

[150] Letter from 60 Members of Congress, to Hon. Tom Wheeler, Chairman, FCC, MB Docket 16-42 (May 5, 2016).

[151] CALinnovates Comments at 2.

diverse programmers."[152] In testimony, Chairman Wheeler has tried to justify the dismantling of MVPD service on the theory that retail providers could then present all minority content, MVPD and online, on the same device. But retail manufacturers do not need a free license to *television* content to promote app and web offerings by minority programmers. Ever since programing has been available online, these tech companies have been able to seek out, promote, pay for, and feature independent or diverse programmers on their retail devices, but they simply have not done so. And even if a retail device were willing to add online programming, that would not address the fundamental economics of online video. Even NPRM proponent Eric Easter, CEO of Blqbox Digital, has admitted that over-the-top video "'should not be seen as a panacea,'" due to "problems with the OTT market includ[ing] the lack of capital to sustain growth while building an audience and the lack of standardization across different viewing devices."[153] The NPRM would not address online programmers' access to capital, or the lack of standardization across CE devices, or require retail manufacturers and app developers to do anything to address those challenges. The NPRM provides no hand up. All it would do is hand over the value of network programming to third parties who will have no obligation to help contribute to or sustain such programming.

But even if the proposed rules would not give consumers more access to online content, the NPRM's proponents suggest that they would help consumers find what they are looking for by having a single video device that can integrate and search content from the entire universe of MVPD and online sources. Google waxes eloquently about retail devices with which "viewers can seamlessly discover and select lawful content online alongside programming from their pay-

[152] League of United Latin American Citizens (LULAC) Comments at 4.

[153] Matt Daneman, *Cable Buying Group Rules Changes Seen in the Works at FCC*, COMMUNICATIONS DAILY (Apr. 26, 2016), subscription service.

TV offerings."[154] But the NPRM does not deliver that vision, because it does not require the disaggregation of OVD content. There is no guarantee that retail devices that use the MVPD information flows could obtain the same disaggregation of content and metadata from other OVDs, especially large OVDs such as Netflix, Amazon, or Hulu. On the contrary, Netflix has intentionally moved in the opposite direction, shutting down its public API that had been open to third party platforms generally and instead moving to business-to-business contractual relationships to define the terms that it seeks to assure delivery of the Netflix service through its app.[155] ARRIS's comments make clear that not all OVDs will simply open their doors for every retail device that seeks their content. ARRIS has sought, unsuccessfully, to persuade Netflix to allow the integration of the Netflix app into some of its set-top boxes that it provides at wholesale to small to mid-sized cable operators.[156]

Proponents also argue, incredibly, that potential new entrants are dissuaded from building new facilities-based broadband networks because of the "excessive costs of procuring video navigation devices."[157] This is clearly false. Any company building a new network to provide broadband and video service would have *more* design flexibility if there were no technology mandate. The reality is that the proposed rules would increase the cost of providing video

---

[154] Google Comments at 3.

[155] *See* DSTAC Final Report at 277 n.47 (DSTAC WG4 at 142 n.47); Janko Roettgers, *Netflix Is Shutting Down Its Public API Today*, GIGAOM (Nov. 14, 2014), https://gigaom.com/2014/11/14/netflix-is-shutting-down-its-public-api-today/.

[156] ARRIS Comments at 8.

[157] *See* Public Knowledge Comments at 54 (arguing that "a competitive app and device market will significantly benefit smaller and new entrant MVPDs" and that the proposal "will save smaller MVPDs time and money while providing their customers with a better experience"); CVCC Comments at 16 (claiming that "[r]obust retail competition would allow manufacturers to take advantage of economies of scale over a larger base of retail navigation device users — ultimately lowering or eliminating costs for new entrants and other small network operators to acquire innovative navigation devices"). The Video Competition Report also claims that the lack of FCC rules remains an impediment to new entrants. *Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming*, Seventeenth Report, MB Docket No. 15-158, DA 16-510 ¶ 219 (2016) ("Seventeenth Video Competition Report").

service. This is why the companies that actually recently built broadband networks, such as the hundreds represented by ITTA, ACA, NTCA and WTA, oppose the NPRM.[158]

Thus, consumers would not save money, or gain access to more content, or receive better broadband under the proposed mandate. Consumers are already enjoying increased choices for the type of navigation device they use to access video services, but that trend is already well underway and does not need any FCC rule to facilitate it. The supposed benefits of the NPRM's proposed rules are a mirage, and certainly do not offset the enormous costs to consumers, content creators, service providers, or networks, or the devastating toll that the mandate would impose on MVPD innovation.

B. There Is Already a "Successor to CableCARD" – Apps Are A Solution and Not a Slogan

CVCC's comments repeatedly contend that there is a need for the FCC to develop a "successor to CableCARD." But the market has already developed the successor – the successor is apps. As demonstrated in NCTA's initial comments, apps are the superior path for assuring the availability of retail devices that present MVPD content as is "offered" and "provided by" the MVPD, as intended by Section 629.

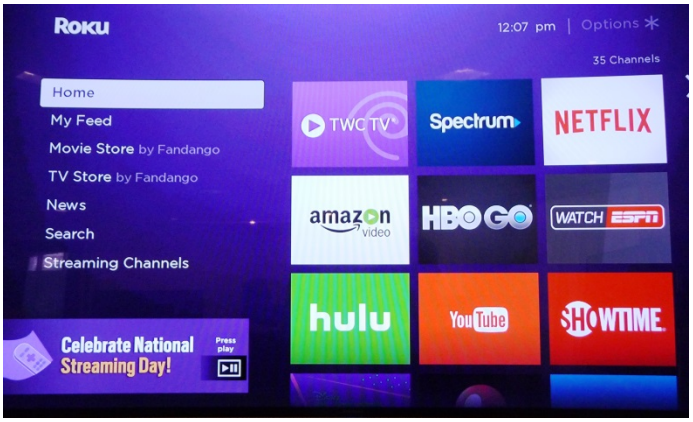
---

[158] *See, e.g.*, ITTA Comments at 2 ("ITTA members are eager to deploy video services in additional geographic markets, but the costs of implementing the NPRM's proposal – especially given already high (and escalating) content costs – could make it prohibitive for them to do so."); *id.* at i (stating that the proposed rules "would only thwart consumer preferences, harm smaller MVPDs – including ITTA members that are relatively new entrants into a challenging and changing video marketplace – and lock into place an obsolete, 20th century, hardware-dependent approach"); American Cable Association (ACA) Comments at 2-3 ("The Commission's network disaggregation proposal will impose substantial costs on MVPDs and produce few, if any, countervailing benefits. Moreover, it is unlawful."); *id.* at 11 (labeling the proposal as "an experiment which is bound to fail but only after first imposing substantial costs on MVPDs, particularly smaller providers, putting the brakes on the innovation that is rapidly occurring in the market and damaging competition provided by smaller MVPDs"); NTCA–The Rural Broadband Association Comments at i ("The Commission should abandon the proposals contained in the NPRM," as they "will inevitably lead to a technology mandate for all providers and impose unreasonable burdens on small MVPDs in particular."); WTA Comments at 3 ("The Commission should not take steps at this time that would disrupt or hinder this progress [in upgrading networks to enable delivery of video programming in IP], including imposition of technological mandates that would require conversions to all-IP delivery before providers have the resources and market conditions to support such transitions.").

1. Apps Enable Retail Devices to Use Distinctive Top-Level User Interfaces Without Disassembling a Service Provider's Offering

The disaggregation proponents claim, notwithstanding actual evidence to the contrary, that a successful retail market cannot be based upon an apps approach because retail devices need to be able to offer distinct user interfaces and experiences to succeed in the market.[159] This argument ignores the proven fact that retail devices or apps do not need to displace the service provider's presentation of its own content and service with their own interface so long as the retail device remains free to have its own top-level interface for organizing content from all providers. This is the approach used by the highly-successful iPad, Amazon Kindle, Google Chromecast, and Roku, among many others.[160]

Figure 1: Roku User Interface with MVPD Apps



As the *Wall Street Journal* puts it, "It is as easy to move back and forth among Netflix, Hulu, Amazon Prime and YouTube as it is to listen to music across Apple Music, Spotify and Pandora.

[159] *See, e.g.*, Public Knowledge Comments at 1-2, 5; TiVo Comments at 4, 14-15.

[160] In addition, hundreds of millions of PCs are running apps – but sales barely register for CableCARD-enabled OCURs that feed linear cable channels into Windows Media Center. In 2015, Microsoft abandoned Windows Media Center.

… Apps for Netflix, Hulu and HBO Now sit next to iTunes on Apple TV."[161] They use myriad other features to attract consumers while permitting service providers to present their own respective services, and these devices have outsold TiVo by a wide margin.[162]

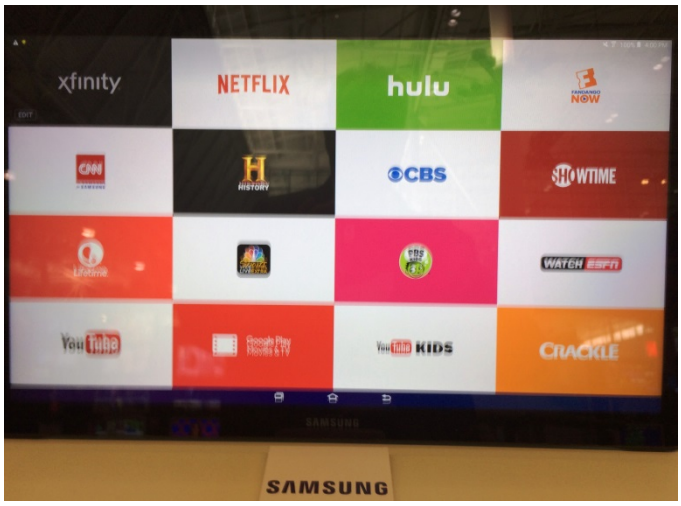


Figure 2: Samsung Galaxy View User Interface with Apps

CVCC offers no evidence at all in support of its claim that accommodating multiple MVPD apps would be "prohibitively expensive" for retail devices.[163] Roku's offering of 3,400 channels represents support for 3,400 apps. The Android app store supports more than 2 million apps.[164] As the DSTAC Report explained, due to "a high degree of commonality" across various app-based approaches, the apps proposal "enables retail device manufacturers many choices for how to receive MVPD services."[165]

---

[161] Miriam Gottfried, *Apple: Why It Hasn't Won the TV War*, WALL ST. J. (Jan. 25, 2016), http://www.wsj.com/articles/apple-why-it-hasnt-won-the-tv-war-1453739527.

[162] NCTA Comments at 7.

[163] CVCC Comments at 36.

[164] *See Number of Available Applications in the Google Play Store from December 2009 to February 2016*, STATISTA, THE STATISTICS PORTAL (last visited May 19, 2016), http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/ ("The number of available apps in the Google Play Store surpassed 1 million apps in July 2013 and was most recently placed at 2 million apps in February 2016.").

[165] DSTAC Final Report at 263 (DSTAC WG4 at 128).

Roku's comments explain how it "and other competing device manufacturers have successfully preserved their own user interface without the necessity of" displacing the needs of its content providers to maintain control over the presentation of their content:

> To simply hand over the user interface of a video service to an unaffiliated third party would be a significant disruption to the industry that would also impact content owners, advertisers, consumers, and others, and would be inconsistent with the successful model that has emerged in the marketplace … User interface provides a critical vehicle for MVPD signups, content discovery, subscriber retention and revenue, each of which can impact the profitability of the video service. User interface is also a vital opportunity for MPVDs to offer step-up options from low-price, entry-level packages. A common practice is to offer low-price entry-level video packages, and then sell step-up options within the user interface. Indeed, the entry price option may be a loss-leader, so the loss of control over user interface may lead to the loss of ability to offer discounted service while promoting additional services, with the net result being that prices may rise. As a result, rules that sever MVPDs from the user interface could lead to a reduction in low-price packages, or lead video distributors to pursue additional revenue streams from consumers to make up the lost revenues derived from the user interface. In this regard, a potential unintended consequence of the Commission's proposed rules could be increased costs to consumers.[166]

2. MVPD Support for Apps Continues to Expand

Public Knowledge claims that the Commission should not rely on apps because MVPDs have not yet created apps for all the platforms and devices that consumers own and use.[167] But MVPDs have invested substantial resources to make their apps available on more than 460 million customer-owned devices in the United States — with two-thirds of the retail devices supporting apps from all of the top 10 MVPDs.[168] Furthermore, as DSTAC noted last year, the trends in app development in recent years "demonstrate[] the continued expansion of MVPD

[166] Roku Comments at 3, 14.

[167] Public Knowledge Comments at 18. TiVo similarly cautions that "apps for consumer devices can also be withdrawn at any time." TiVo Comments at n.9. Some apps do sunset as consumer interest in using a platform for video wanes. Xbox 360, launched a decade ago, was succeeded by Xbox One in late 2013. In 2015, Microsoft terminated support for the Media Center PC, for which the CableCARD OCUR was designed, and Google sunset YouTube apps on older devices. DSTAC Final Report at 283 (DSTAC WG4 at 148). But new platforms rise, like HTML5. MVPDs have demonstrated a commitment to expanding the reach of apps that reach a significant number of their customers.

[168] NCTA Comments at 11 (citing DSTAC Final Report at 208, 263 (DSTAC WG4 at Tables 8, 9)).

apps in response to consumer and competitive demands."[169] It is ludicrous to suggest that MVPDs that have invested in developing apps that can run on millions of retail video devices, and have encouraged their customers to download tens of millions of their apps, will turn around and look for excuses to shut them down.[170]

The NPRM's proponents resort to a series of baseless talking points and fallacies in their efforts to dismiss the transformational impact of apps on the video marketplace. CFA claims "Cable companies hold the exclusive domain over how content is transmitted to the public," and that the market reflects "absence of competition and the abuse of market power" by MVPDs.[171] The reality is that the economic paper on which CFA bases its claims is 25 years old – taken straight from CFA's efforts that led to passage of the Cable Act in 1992.[172] Ninety-nine percent of homes have access to at least three MVPDs and thirty-five percent have access to four MVPDs.[173] American audiences today can find nearly all premium films and premium television series online and can choose among more than 115 online services to legally access television and film content over the Internet.[174] Viewers used these services to access 66.3 billion television episodes and 7.1 billion movies in 2014.[175] Apps from TV providers are already available (right alongside apps from streaming providers) on more than 460 million consumer-owned devices.

---

[169] DSTAC Final Report at 297 (DSTAC WG4 at 162).

[170] NCTA Comments at 11.

[171] CFA Comments at 9.

[172] *Id*. at 2 ("CFA was active in supporting the Cable Consumer Protection Act in 1992, which provides the basis for some of the economic analysis in Attachment A")."

[173] *Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming*, Sixteenth Report, MB Docket No. 14-16, 30 FCC Rcd 3253 ¶ 31 Table 2 (2015) ("Sixteenth Video Competition Report").

[174] *See supra* at 4, 39; *see also* MPAA/SAG-AFTRA Comments at 2.

[175] MPAA/SAG-AFTRA Comments at 2.

Year-over-year viewing via MVPD apps more than doubled in 2015; with 40% of MVPD subscribers using "apps" to view their subscription content.[176]

They reiterate the talking point that 99% of consumers have no choices for set-top box alternatives. The claim that "99%" of consumers are required to use set-top boxes is a rhetorical artifice achieved only by ignoring the millions of other devices with which consumers receive their multichannel services.

CFA's only retort is that all this evidence showing that the "broader MVPD market is competitive is merely an effort to divert attention."[177]

The Video Competition Report, which was released during this rulemaking comment cycle without review by the voting Commissioners, has itself offered similar misstatements. The Commission's talking point is that MVPD apps focus on serving mobile devices,[178] when the reality is that MVPD apps already serve streaming boxes, Smart TVs, and gaming stations.[179] Expansion towards HTML5 apps can serve even more TVs.[180]

The Commission's next talking point is that among MVPDs "only five have applications for the Microsoft Xbox 360, despite its being more common than either tablet."[181] The reality is that those MVPD apps include AT&T/DirecTV and some of the other largest MVPDs. All of the top 10 MVPDs have apps on the far more numerous Android and iOS devices.[182] And as to

---

[176] *See* NCTA Comments at 12.

[177] CFA Comments at 20.

[178] Seventeenth Video Competition Report at ¶ 217.

[179] *See* NCTA Comments at 17; *supra* at 43. The FCC even claims that only one MVPD supports Roku, when in reality both Time Warner Cable and Charter appear on Roku today and Comcast has announced itself as the third MVPD to support the device.

[180] Smart TV platforms that support HTML5 as a platform for TV applications include: Android TV (Sony), Tizen (Samsung), Firefox OS (Panasonic), and webOS (LG). *See* Technical White Paper at n.97; AT&T Comments at 10.

[181] Seventeenth Video Competition Report at ¶ 217.

[182] Over 135 million Android devices, and 95 million iOS devices were reported in DSTAC, compared to 48 million Xbox 360s.

mobile – the very same report explains that the increased screen size on phones alone makes them practical higher resolution video viewing devices,[183] and current tablets (like the Samsung Galaxy View shown in Figure 2) clearly serve as televisions.[184]

MVPDs have powerful incentives for supporting apps: they reduce capital expenditures, maintenance costs, truck rolls and installation visits; they can be updated rapidly; and they meet growing customer demand.[185] In the past, MVPDs prioritized the most popular platforms for their apps to meet demonstrated consumer demand, but DSTAC reported 15 supported platforms in 2015 with two-thirds of the retail devices supporting apps from all of the top 10 MVPDs. MVPD support for apps only continues to expand. Comcast's new Comcast Xfinity TV Partner Program offers a standardized app open to all platforms that support an HTML5 browser, and dozens of companies have responded to Comcast just in the first weeks since the program was announced.[186]

---

[183] Seventeenth Video Competition Report at ¶ 225.

[184] Xiomara Blanco, *Samsung Galaxy View Review: Biggest Samsung Tablet Ever, Smallest TV in Your House*, CNET (Nov. 6, 2015), http://www.cnet.com/products/samsung-galaxy-view/.

[185] NCTA Comments at 11-16; DSTAC WG4 at 162 ("the evidence demonstrates the continued expansion of MVPD apps in response to consumer and competitive demands "); 167 ("Apps give MVPDs the tools to keep enhancing service continuously without awaiting industry consensus, standards, or rule changes; to create value and consumer recognition of that growing value from their (branded) service provider; and to help retain them as customers. Apps give MVPDs the tools to innovate with new technologies, to shape and reshape their offerings to meet changing consumer demands."); 171 ("Multichannel service is no longer a simple broadcast video service, but a complex interaction of licensed content, network, security, content protection, hardware, software, licensed metadata, diagnostics, application data synchronized with content, UI, advertising, ad reporting, audit paths, etc. The technology varies across platforms and changes continuously without awaiting industry consensus, standards, or rule changes. Apps allows [sic] delivery of this service to a wide variety of CE devices and platforms, none of which are built to a common standard. Reducing MVPD service to unimproved broadcast channels sacrifices decades of improvement and frustrates the continued innovation among competing MVPDs that keeps driving more innovation. … Consumer demand varies and evolves, and competitors have the right to innovate with new technologies, to add value-added services, to shape and reshape their offerings to meet changing consumer demands. Diversity and an apps approach enables MVPDs to enhance their networks over time to increase network capabilities, such as increased capacity, device addressability, security, reliability, energy efficiency, quality of service, and operational efficiency. Application and feature updates are occurring multiple times a month, effected with an application update. The changes do not await agreement on a new protocol or standard. Applications allow the MVPD to advertise and promote these new features through their applications.").

[186] *See* Xfinity, The Xfinity TV Partner Program: Bringing the Xfinity Experience to More Consumer Devices and TV Screens, https://developer.xfinity.com/cableapp (last visited May 11, 2016); Mark Hess, *Comcast Seeks TV and*

3. The Functionality of Apps Continues to Expand

Video Offerings. TiVo claims that "[t]he functionality of apps is typically limited and generally does not give consumers access to all of the channels they get from their set top box."[187] On the contrary, MVPD apps continue to grow. Only five years ago, Time Warner Cable and Viacom were locked in litigation over TWC's delivery of service to an iPad. Today, Time Warner Cable apps provide 300 linear channels, video-on-demand, and a TWC-supplied guide on Roku and eight other retail platforms. Comcast's Xfinity TV apps offer Comcast's full linear channel lineup, VOD, and Cloud DVR capability on smartphones, tablets, and PCs and Macs in most of the homes in its footprint; and it just announced partnerships with Roku and Samsung that will enable Comcast customers to access their live and on demand programming, including local broadcast, cable and premium networks, Public, Educational and Governmental (PEG) channels, and cloud DVR recordings in the home using only Roku Smart TVs and Roku streaming players, and certain models of Samsung Smart TVs without any leased Comcast set-top box.[188] These Comcast apps will "offer consumers viable substitutes to a full-featured, leased set-top box."[189]

High Resolution. Public Knowledge claims that apps are lower resolution; but VidiPath delivers apps in HD, as does RVU. RVU even implemented 4K.

Other Consumer Electronics Partners to Bring XFINITY TV Cable Service to More Retail Devices, COMCAST VOICES BLOG (Apr. 20, 2016), http://corporate.comcast.com/comcast-voices/comcast-seeks-partners-to-bring-xfinity-tvcable-service-to-more-retail-devices.

[187] TiVo Comments at n.9.

[188] Shalini Ramachandran, *Comcast Fires Back at FCC by Making TV Service Available Without a Set-Top Box*, WALL ST. J. (Apr. 20, 2016), http://www.wsj.com/articles/comcast-fires-back-at-fcc-by-making-tv-service-available-without-a-set-top-box-1461188283 (explaining that Comcast made "its full TV lineup available on Roku devices and Samsung smart TVs for the first time, without requiring customers to lease its proprietary box").

[189] NPRM at ¶ 16.

Recordings. TiVo yet again repeats the false argument that MVPD apps do not "allow consumers to record programs for viewing later."[190] On the contrary, MVPD apps allow subscribers to use their smartphones, tablets and Rokus to record to the cloud.[191]

Easy Log On. Public Knowledge seeks to discredit apps as unfriendly to consumers, claiming that they require multiple log-ins for every channel, "hardly a consumer-friendly mechanism for accessing content that consumer [sic] is already paying for, particularly when compared to the simple channel guide consumers are accustomed to using."[192] The reality is that an MVPD app either offers an easy log in to the full guide with all channels listed, or (as is the case with Charter Spectrum on Roku) auto authentication without the need to enter a user name and password when accessing the app. Public Knowledge has conflated individual programmer apps – that make channels available direct from the programmer – with MVPD apps.

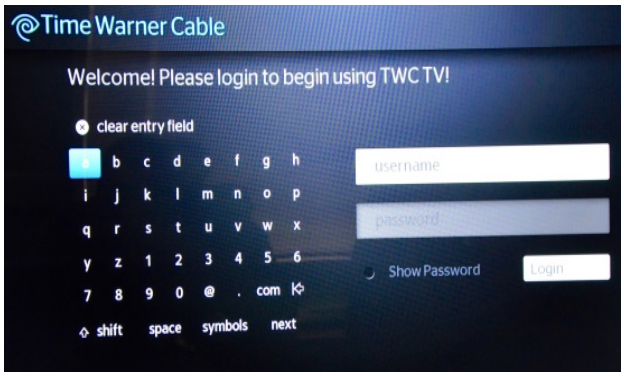


Figure 3: Simple Log-in to TWC App, providing access to all channels

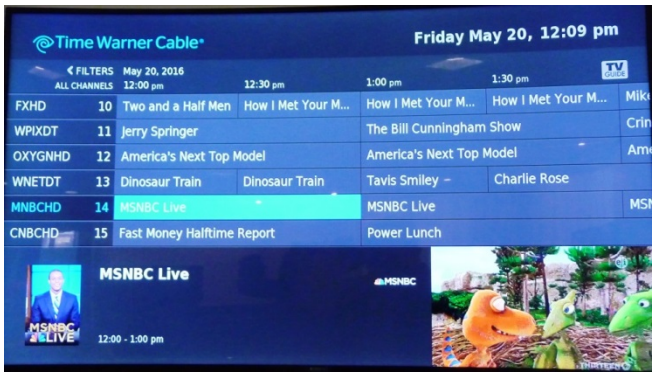


Figure 4: TWC Guide once "Clicked" on Roku

[190] TiVo Comments at n.9.

[191] NCTA Comments at n.156; Letter from Neal M. Goldberg, Vice President and General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, MB Docket 15-64 (Nov. 30, 2015) (describing how a VidiPath client could include a local DVR and a top level app to record to a hard drive).

[192] Public Knowledge Comments at 27.

Programmers offering single subscription channels must be able to authenticate the user as an authorized viewer, but that does not affect the ease of accessing MVPD apps on retail devices.

Integrated Search. TiVo claims that "[p]roprietary MVPD apps generally do not allow consumers to search across MVPD and OTT services."[193] Putting aside the fact that the proposed FCC rules would not force OVDs to permit integrated search of their content, the market is already creating content discovery tools that draw on multiple sources. Roku enables

Figure 5: Integrated Search of TWC and OVDs

consumers to search Time Warner Cable content and online content from a common interface. The Samsung platform announced at CES 2016 supports cross-app search and "smart remotes" that remember which HDMI input to use. Co-branded guides, such as one shared by Suddenlink and TiVo, support integrated search. Business-to-business deals allow Comcast video on demand to be searched by a TiVo, and a separate agreement between TiVo and Netflix helps consumers search both at the same time. Cable operators are exploring integrated search that may include other apps on leased set-top boxes. Integrated video search has just been introduced to iOS 9, and is supported in Android, Apple TV OS, and Amazon Fire TV, all using different approaches.

[193] TiVo Comments at n.9.

Integrated search is developing organically in the market right now, without the need for an FCC set-top box mandate.

Portability. TiVo complains that "[p]roprietary apps are also not portable; i.e., they will not work with another provider's network."[194] But there is no need for an MVPD app to be portable to another MVPD. MVPD apps are free, and if a consumer switches providers they can just download their new MVPD's app. The notion of portability for an MVPD app also makes no sense, since the purpose of the app is to access the particular MVPD's service, just as it makes no sense to complain that the Amazon app cannot be ported to YouTube – of course they can't, because they are different services.

In sum, none of the criticisms of apps submitted in comments in this proceeding undermine the clear evidence in the record that consumers, content owners, standards bodies and industry worldwide have embraced apps as the future of TV, and that there is no better path than apps for the Commission to follow in seeking a simple, effective means of achieving the statutory purpose of Section 629.

C. The Proponents Failed to Demonstrate that the Proposed Rules Would Not Jeopardize the Security Of MVPD Services and Networks

Section 629(b) requires that the FCC "shall not prescribe regulations under subsection (a) of this section 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."[195] Despite this unambiguous limitation on FCC authority, neither the NPRM nor the supposed "clarifications" offered by its few supporters propose a method of protecting the three naked information flows that would not jeopardize

[194] TiVo Comments at n.9.

[195] 47 U.S.C. § 549(b) (emphasis added).

security of the entire multichannel video ecosystem, or interfere with measures to combat theft of service. As NCTA detailed in its Comments and Technical White Paper, the proposed rules would bar MVPDs from relying upon an end-to-end trust infrastructure, agreements, and MVPD-provided apps operating in a trusted application execution environment, all of which are essential to security. That infrastructure allows the code provided by the MVPD to operate in a trusted application execution environment *within* the app that runs on the device, to interact securely with the network, and to present service in accordance with the required license obligations and security requirements for distributing multichannel video programming and other services and enforcing the legal rights of each service provider to prevent theft of service.

Chairman Wheeler has said that delivering content "safely" to a third-party device within the trust infrastructure and through MVPD apps (such as through a Comcast app on a Roku or a Samsung TV) "is proving [his] point" that you can do so outside that trust infrastructure and without an MVPD app without "all these other horrible things" like loss of security, privacy, copyrights and the like.[196] But the technical reality, evidence, and record is quite clearly to the contrary: Without that trust infrastructure and without an MVPD app, security is jeopardized and theft of service invited.[197]

Rather than addressing the undeniable gap between the robust security that MVPDs currently are able to provide via app-enabled trust infrastructures, and the limited security proposed for the three information flows, proponents of the NPRM instead focus on additional ways that the FCC might further constrain MVPDs' ability to protect service.

---

[196] Jon Brodkin, *Tom Wheeler: Comcast's TV App Proves the FCC Is Right about Set-Top Boxes*, ARS TECHNICA (Apr. 29, 2016), http://arstechnica.com/business/2016/04/tom-wheeler-comcasts-tv-app-proves-the-fcc-is-right-about-set-top-boxes/ (emphasis added).

[197] NCTA Comments at 80-81; Technical White Paper at 14-21, 30, 36.

Further narrowing security options. TiVo proposes to narrow MVPDs' security options even further than the NPRM suggests. It urges that the Commission forbid any MVPD from using any security solution for the information flows that is not used by multiple MVPDs, that is not deployed to 15 million subscribers, or that makes use of a specific hardware root of trust.[198] In one fell swoop, it would disqualify use of the MVPD equivalent of Apple's Fairplay (which is exclusive to Apple), the downloadable security already deployed by two cable operators, as well as any security solution from a new security vendor seeking to break into the market with its first U.S. customer, regardless of its quality. It then adds that however security is implemented in the three information flows, MVPDs should be confined to "*no more than a small number of solutions*."[199]

This claim ignores both the danger of creating single points of failure and the basic design of the modern apps-based security system that promotes helpful diversity and competition in security solutions. One of the most basic tenets of security design is that single points of failure undermine overall security. This was one of the major points of agreement during the DSTAC process, which reached consensus on the principle that any recommendations should "avoid rigid and/or single implementations (one-size-fits-all) that significantly limit[] innovation, competition, or increase[] security risk."[200] As Verimatrix points out, "[t]here have been numerous attempts in the past to standardize security and all have faced one intractable problem – they create single points of attack. Diversity is an important aspect of security – if one system

[198] TiVo Comments at 19 ("[T]he Commission should require that any Compliant Security System be supported by multiple MVPDs, in aggregate serving at least 15 million subscribers without being tied to an MVPD-specific Trust Authority or chipset or other hardware requirement.").

[199] *Id*. at 18 ("The Commission should … seek to ensure that MVPDs converge on *no more than a small number of solutions* to ensure that competitive device manufacturers and app developers are not faced with having to produce different products for each MVPD.").

[200] DSTAC Final Report at 76 (DSTAC WG3 at 18).

fails, it doesn't necessarily bring down the other systems."[201] It warns: "[t]here is already the danger that a regulation in this space will lead to a de facto Compliant Security System standard that increases the threat of a single point of failure. Any regulations should in no way impair normal market forces that are currently in play to try to counter this risk. The system will be more secure with a diversity of security solutions…. [T]he Commission was right to refrain from standardizing a single Compliant Security System solution and should resist any tightening of its proposed rules that would lead to less diversity in security."[202]

Rather than attempting to confine MVPDs to single points of failure, the apps-based market has moved towards common encryption to promote diversity and allow for rapid responses to hacks. Common encryption allows the content to be encrypted once but decrypted by different keying systems, allowing for use of multiple DRMs and even the replacement of one DRM by another in response to failure of security. That is why the World Wide Web Consortium ("W3C") specifically chose to implement common encryption for its web streaming standards in a way that supports multiple keying systems.

Narrowing the available security solutions needlessly weakens security.

Mandating Key Sharing at the Weakest Link. Key sharing is an important tool, but , as security vendor Verimatrix makes clear, that tool needs to remain within the control of the MVPD responsible for the secure distribution of the programming.[203] CVCC seeks to further weaken security by mandating key sharing with two systems whether or not an MVPD has selected them for security: Google's Widevine and Microsoft's PlayReady.[204] Widevine is

---

[201] Verimatrix Comments at 8.

[202] *Id*. at 9.

[203] *See* Verimatrix *Ex Parte*.

[204] CVCC Technical Appendix at 4 ("Common Encryption should be used for DRM, with support for either Widevine or Microsoft PlayReady DRM clients for key exchange. Alternate DRMs may *also* be used, as long as

affiliated with the MVPD Google Fiber and would be disqualified as a content protection system under the terms of the NPRM. That leaves one specific point of failure – a weak link independent from the Compliant Security System(s) selected by the MVPD but that would nonetheless be capable of jeopardizing the security of every MVPD's services via a single breach. If it is hacked, all systems are exposed.[205] This lowers the overall robustness of the security regime.

Increasing Vulnerability of DRM License Server. The NPRM already weakened security by proposing to relocate the DRM license server outside of the MVPD firewall. CVCC goes still further and would require the IP address of any DRM license server(s) to be advertised,[206] thereby exposing those servers even further to hackers and undermining overall security.[207]

Continued Indifference to User Authentication. The NPRM includes no element of user authentication, which is essential to protect against theft of service.[208] In a long pattern of changing and flip-flopping on proposed technical "solutions,"[209] CVCC proposes a new approach that provides only the appearance of user authentication, but not the reality. Translated from the obfuscation endemic to its "technical" proposal, CVCC proposes that users enter a log in on a third-party registry, which CVCC likens to how consumers log into authenticated

---

they utilize Common Encryption *and also provide support for key exchange with either Widevine or Microsoft PlayReady DRM clients*.") (emphasis added).

[205] Technical Analysis at 12.

[206] *See* CVCC Technical Appendix at 4 ("When DRM is used for content protection, the DRM license server should be specified in the DASH manifest or be specified in the CDS using the *DRMInfo:foreignMetadata* property. When an in-home MVPD device is used for providing the Service Discovery Interface, then it also must act as a proxy to the DRM license service for the DRM key exchange and perform all authentication with that license server itself.").

[207] Technical Analysis at 13.

[208] *See* NCTA Comments at 97; Technical White Paper at 21; Technical Analysis at 14-15.

[209] *See* Technical Analysis 4-6, 7-10, 11-12; *see also id*. at 4 ("If any of the device proposals, including the conceptual one advanced in the NPRM, were technically feasible, it would have been possible for their proponents to put forth a consistent and stable proposal.").

programmer web sites like HBO.[210] But, like the NPRM, CVCC ignores a critical part of how security works within a trust infrastructure. An MVPD is willing to trust a log in through its program licensors and suppliers because they are partners in contract and equally invested in security and preventing theft of service. The devices that the CVCC proposal envisions, by contrast, would be located outside of that trust infrastructure, outside of any contract, operated by companies that have announced their hostility to the bounds of license or copyright and that are positioned beyond the reach of FCC jurisdiction. Without the trust infrastructure and without an MVPD app, security is jeopardized and theft of service invited in that model.[211]

DTCP is Still Too Limited a Solution. Proponents of the FCC rules inevitably return to the position that some version of DTCP link-layer protection might serve as one – if not the only[212] – acceptable form of content protection. But as NCTA and others have demonstrated,[213] DTCP continues to lack the features and capabilities that programmers demand for their high-value content today, and its development history strongly suggests that it would not be able to respond to new business plans and security threats in a timely fashion going forward.

DTCP remains a method to protect point-to-point (that is, "unicast") links between devices connected either directly (e.g., a set-top box connected to a recording device via an IEEE-1394 cable) or over a home network. (That explains why DTCP-IP limits the number of connected devices to 34 and requires localization.) As a result, if an MVPD were to choose (or was required by regulation) to utilize DTCP to protect content delivered from the cloud, it would

---

[210] CVCC Technical Appendix at 5 ("[a]uthentication … should be done via techniques similar to what MVPDs use for TV Everywhere login (i.e., either automatic or via webpage login with their MVPD credentials).").

[211] Technical Analysis at 14-15, 17.

[212] CVCC Comments at 38-40; Technical Analysis at 4, 8-9.

[213] *See* NCTA Comments at 128; NCTA DSTAC Comments, MB Docket No. 15-64 (Oct. 8, 2015) at 25; NCTA DSTAC Reply Comments, MB Docket No. 15-64 (Nov. 9, 2015) at 27, 28-29, 35-36 ("NCTA DSTAC Reply Comments"); Letter from Rick Chessen, Sr. V.P. Law and Regulatory Policy, NCTA, to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Jan. 15, 2016) at 2-3.

not only have to simulcast the Content Delivery Interface (i.e., provide DTCP-protected streams in addition to those streams serving leased/legacy devices) – it also would have to deliver those DTCP-protected streams via unicast wasting substantial amounts of bandwidth and would far exceed not only available broadcast bandwidth, but total bandwidth available on today's systems.[214]

DTCP has been very slow to evolve. By way of example, DTCP+ has never been deployed, DTCP 2 was never finished and has not been deployed, and DTCP-HE, to our knowledge, at this point is nothing more than "slideware."[215] Because DTCP has not been able to replicate the tools and capabilities offered by competing apps and DRMs, neither content providers nor distributors consider DTCP, by itself, to provide a sufficient level of security.[216] As one example, two full years after DIRECTV launched its Ultra High Definition service to consumers, DTCP still is unable to provide a level of security for the highest-quality video formats available (e.g., UHD, 4K) that is deemed sufficient in the video marketplace.[217] Even if it "fixed" that tomorrow, it would remain years behind the nimble development of other security solutions.

Unlike DRMs, DTCP does not support common encryption. Common encryption – a technique that CVCC's proposal expressly encourages[218] – allows a distributor to encrypt content only once, while still supporting multiple DRMs and the ability to switch quickly to rival DRMs (for example, in response to a security breach). Common encryption thus provides a number of

[214] *See* Technical Analysis at 9 ("DTCP is local link-protection technology that caps the number of devices at less than 35, restricts devices to a set proximity, and it too does not scale to the cloud. DTCP assumes a point to point connection in the home; scaling to a multi-point to multi-point architecture does not scale, even if device number and proximity limitations were relaxed."). DTCP-2 has not been released and does not change these restrictions.

[215] *Id*. at 13.

[216] *See* NCTA Comments at 128.

[217] *See* NCTA DSTAC Reply Comments at 35.

[218] *See, e.g.*, CVCC Technical Appendix at 4 (stating that "[c]ommon Encryption should be used for DRM").

benefits, including: (a) it eliminates the need to simulcast duplicate versions of the same content protected using different DRMs, (b) it uses bandwidth far more efficiently, and (c) it promotes competition in the DRM/security market.[219]

Ineffective Robustness and Compliance Rules. CVCC would reduce security still further by proposing robustness and compliance rules (the rules that define resistance to hacking attempts and the authorized "outputs" of content from a security system) that are archaic, wrenched from context, and detached from any trust infrastructure.

CVCC proposals profess to rely in large part on the DFAST license, but, as NCTA previously explained, the DFAST license was developed to address a much more narrowly scoped issue: securing the one-way delivery of linear cable content. Moreover, it was only intended to serve a transitional role, as both the cable and CE industries had committed to work on an apps-based solution for two-way capabilities.[220] DFAST thus did not address interactive components of cable operators' services. And it certainly did not provide a license for that protected content.[221]

CVCC extracts the robustness and compliance rules from the DFAST license as a supposed model.[222] But security infrastructures and content rights have changed since DFAST was written in 2002. For example, DFAST does not have a provision for out-of-home streaming rights that are defined by affiliate agreements today, nor does it provide robustness rules for the

---

[219] *See* DSTAC Final Report at 82-83 (DSTAC WG3 Report at 24-25).

[220] That app approach was agreed to be used for two-way cable service by all of the major CE manufacturers for two-way cable service: Sony, Samsung, Panasonic, LG Electronics, Funai (operating under the consumer-facing brand names Philips, Magnavox, Sylvania, and Emerson), Digeo, ADB, Echostar, and Intel. Two-way license warranties explicitly required services to be delivered the way they are on cable boxes, with all ads, and "no 'disaggregation' of the cable services is permitted." Virtually all other video distribution platforms have adopted an app-based approach: iOS, Android, PCs, Macs, Smart TVs, Xbox, PlayStation, Roku, HTML5 and VidiPath. Technical White Paper at 6, 54.

[221] *See* NCTA Comments at 61; MPAA/SAG-AFTRA Comments at 15.

[222] CVCC Comments at 41-42.

cloud storage that CVCC proposes.[223] As MPAA notes, all approved technologies have been for in-home use only.[224] Apps, agreements, and a trust infrastructure that enforces license rights are used for security today, but CVCC wants none of that. Like the NPRM, it would remove the agreement, privity, content provider third party beneficiary rights, and device testing and certification that are essential to a chain of trust.[225]

CVCC's proposal has no Intellectual Property hook on which to condition compliance and no licensing authority to enforce it. It calls for "consultation" over changes in robustness rules – but in the context of a proposed rule that excludes service providers who seek to secure content from even having a license or contract on which to consult.[226] Excluding MVPDs from licensing and security agreements would (a) run counter to the trust infrastructure-based, industry standard approach to security, and (b) undermine MVPDs' need to secure content if they are to obtain distribution rights in the first place.[227] CVCC instead would refer all disputes for resolution to the FCC[228]—a body that has never written, adopted or enforced a security license agreement for commercial video content, and has assiduously avoided assuming that role

[223] CVCC proposes that retail apps and devices could store content in an unlicensed cloud. CVCC Comments at 35. That would effectively transform every third party into an unlicensed VOD server.

[224] *See* MPAA/SAG-AFTRA Comments at 9-10.

[225] Such tools are especially needed with respect to devices over which the FCC has disclaimed jurisdiction to enforce requirements. *See* ARRIS Comments at 15 ("DRMs and MVPDs' app configurations work in tandem to create a trusted environment for content. For example, DRMs may not always convey output controls, but MVPDs implement these restrictions in their apps. This trusted environment would be jeopardized if third parties, who are not parties to programming agreements, can create their own derivative services using their own interfaces that strip out the security features embedded in MVPD apps."); Verimatrix Comments at 20 ("Device compliance must be certified and may need to be certified by an independent test lab."); Technical White Paper at 5-9. By contrast, CVCC seeks to require some ill-defined certification testing for MVPD outputs of information flows, notwithstanding that MVPDs have operated successfully under direct authority of myriad FCC rules for accessibility, emergency alerts, moderation of loud commercials, children's programming, and much more without such unnecessary requirements.

[226] CVCC Comments at 42.

[227] Verimatrix Comments at 11 ("MVPDs should not cede their responsibility and authority for the overall security of their distribution network.").

[228] CVCC Comments at 43.

even at the height of plug and play and broadcast flag regulation.[229] This would be a complete abrogation of an effective security regime.

As the MVPD industry repeatedly has explained, distributors of video today utilize a combination of security resources that include DRMs and apps that they develop and publish to establish an overall trust infrastructure that protects their services and supports new rights and business models.[230] This is true for MVPDs subject to regulation under Section 629, competing OVDs, and the CE industry generally. One need only look to recent marketplace developments – iOS, W3C, Roku, and everything showing at CES 2016 – to realize that the world of video fully has embraced DRM. The NPRM approach – to limit security and remove retail devices from the trust infrastructure – would uniquely prevent MVPDs from using the most innovative security. OVDs, by contrast, would remain free to experiment with other security systems, thereby exploiting disparate regulatory treatment in order to obtain high-value content and support new business models that MVPDs could not.

There is a common root to the security failures of the Commission's proposal. The NPRM and its supporters have attempted to decouple content security – whether link protection (DTCP) or DRM – from MVPDs' overall video ecosystems. As NCTA explained at length in Comments and associated technical submissions, MVPD security hinges on the integrity and

[229] In the 2003 Plug and Play Order, the FCC chose not to adopt or administer DFAST, and not to agree to any specific enforcement role beyond its general complaint procedures and review of disputed output decisions. *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Second Report and Order and Second Further Notice of Proposed Rulemaking, CS Docket No. 97-80; PP Docket No. 00-67, 18 FCC Rcd 20885 (2003). In the Broadcast Flag Order, the FCC certified a wide variety of security regimes and a variety of licensing agreements and specifically decided not to dictate license terms. *Digital Broadcast Content Protection*, Report and Order and Further Notice of Proposed Rulemaking, MB Docket No. 02-230, 18 FCC Rcd 23550 (2003).

[230] *See, e.g.,* NCTA Comments at 68-72, 90-106; Technical White Paper at 5-9; Comcast Comments at 89-91; AT&T Comments at 45-46.

robustness of the trust infrastructure.[231] A content protection system that is decoupled from a trust infrastructure does not provide security or prevent theft of service. Indeed, the entire NPRM proposal is founded on the notion that retail navigation devices are entitled to the unfettered and uncompensated use of the "content" and other intellectual property that is supposed to be protected by the security and anti-theft regimes protected by Section 629(b). Any rule premised on those fundamental lapses – however its proponents try to dress it up or patch it up – would fail to meet the basic requirement of Section 629(b) that the FCC not *jeopardize* security or impede providers' legal rights to prevent theft of service.

D. CVCC's Latest Amendments to Its Supposedly "Complete" Proposal Serve Only to Illuminate Its Inherent Flaws

As has long been the pattern, proponents of the NPRM pretend that three unbundled information flows can deliver MVPD service using "mostly" "off the shelf" technology in "common use" today requiring "no changes" in MVPD networks and "nothing new" beyond "existing standards and technology 'borrowed' from CableCARD."[232] But with each iteration they change the supposed 'existing' technologies, call for new inventions, and flip flop on proposal after proposal.

1. Proponents' Submissions Continue a Tradition of Constant Changes and Flip Flopping in Technology Proposals.

During the DSTAC debate, they suggested 38 protocols, only some of which in fact exist; the others would have required additional invention, and all were roundly critiqued. In their October 20, 2015 *ex parte* submission, they dropped 31 of the original 38 protocols, kept 7

[231] *See, e.g.,* NCTA Comments at 33-34, 78, 90-93, 98; Technical White Paper at 5-9, 16.

[232] *See, e.g.*, Public Knowledge Comments at 55; CVCC Comments at 6, 9; *see also* Public Knowledge Comments, MB Docket No. 15-64 (Oct. 7, 2015) at 18; Hauppauge Comments, MB Docket No. 15-64 (Oct. 8, 2015) at 2.

(mostly minor protocols), and introduced 10 new ones. They were again roundly critiqued. As described by NCTA and others:[233]

- It required a second box in the home to accommodate two of its proposed technologies, UPnP and DTCP[234]
- It called for UPnP approaches *not* "in common use by MVPDs today," never proved through common adoption across all MVPDs, with many never deployed at all.[235]
- It relied on supposed DLNA EPG Guidelines that were abandoned by DLNA, were never implemented, and are completely unproven.[236]
- It proposed content protection that has never been deployed.[237]
- It would have required MVPDs to serve unauthenticated devices.[238]
- Contrary to CVCC claims,[239] the proposal could not "be described and referenced in accordance with the tools comprising DLNA CVP-2" nor would it "draw on independent certification tools and bodies already in existence."[240] It did not "most

[233] *See, e.g.*, NCTA Comments at 121-122; AT&T Comments at 20-21.

[234] *See* Technical Analysis at 9, 15; NCTA DSTAC Reply Comments at 27 (explaining that the device proponents' "new proposal has replaced the interfaces proposed in DSTAC with home networking protocols based on UPnP and DTCP that would make cloud delivery impossible," and that "[t]he new proposal would also require MVPDs to provide a government-designed intermediary device used to interface with retail devices in the home, locking consumers into more (not fewer) boxes with their associated lease payments and higher energy consumption when consumers want a boxless, wireless solution that apps can support on the customers' own devices").

[235] *See* Technical Analysis at 11; NCTA DSTAC Reply Comments at 33.

[236] *See id.*; AT&T Comments at 21.

[237] *See* AT&T Comments at 21; NCTA DSTAC Reply Comments at 33; AT&T Comments, Technical Declaration of Stephen P. Dulac at 7-8 ("DTCP-IP also cannot support delivery of services via the cloud because there is no DTCP-IP solution supporting cloud delivery that content owners have approved. DTLA published a specification for 'DTCP+' about 5 years ago that included some use cases allowing content sharing beyond a local area network. However, to my knowledge, these DTCP+ cloud use cases have not been implemented in practice, nor have they been approved by content owners in bilateral agreements.").

[238] *See* Technical Analysis at 8; NCTA DSTAC Reply Comments at 28.

[239] *See* Technical Analysis at 6-11.

[240] Letter from John Bergmayer, Senior Staff Attorney, Public Knowledge to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Oct. 20, 2015), Exhibit at 1 ("Public Knowledge Oct. 20, 2015 *Ex Parte*").

resemble VidiPath" or use "independent certification tools and bodies already in existence … at minimal burden."[241] It actually gutted VidiPath and called for a diametrically opposite set of new unproven requirements. The supposed independent certification tools and bodies already in existence were actually unproven and not testable by DLNA certifications.

- The proposal would also require major development efforts to create a new hardware device in the home.[242]
- And of course, it suffered the underlying inability to deliver MVPD service, with intellectual property, privacy and regulatory protections assured.

The NPRM nonetheless cites it as an existing solution and makes no mention of these documented failings.

Now, in their Comments on the NPRM, they put forth still another set of proposals and undefined protocols to "augment" what they once claimed was a final, build-to solution. The CVCC Technical Appendix offers yet another set of 17 protocols (existing or to be invented), nine (9) of which (or over half) are newly specified in this proposal. This time, they claim to have identified a collection of existing (or nearly so) technologies that could enable the FCC's proposal.[243] As demonstrated below, however, the same problems remain and each attempt to shore up that list inevitably introduces still more problems.[244]

---

[241] *Id*.

[242] *See* Technical White Paper at 45-46, 49-50; Technical Analysis at 11.

[243] CVCC Technical Appendix at 1 ("The technical references listed below illustrate clearly that existing technologies, with specific minor changes, may be readily formulated to support full compliance with the FCC's objectives and proposed rules. Hence, standards formulation and recognition can and should be expeditious.").

[244] *See* Technical Analysis at 11-16.

2. The Proposal Is Still a Two-Box Solution

First, CVCC's submission resolves the two-box question, once and for all: *a second device would be required*. This has always been true for satellite, and as described in the Technical White Paper it is true for cable as well.[245] Now CVCC explicitly calls for an IP feed[246] which effectively calls for an in home device in systems that have not gone IP. And it calls for UPnP and DTCP,[247] two technologies designed specifically for in-home use – and which, as a result, are incompatible with cloud-based delivery that apps-based approaches could otherwise deliver. The CVCC proposal explicitly refers to "an in-home MPVD device."[248] CVCC may protest that no second box is required, but its proposal says otherwise, and it is clearly quite willing to impose this additional burden (and cost) on unsuspecting MVPD subscribers – so long as it enables unbundled third-party access to MVPD programming.

In its Comments, CVCC implicitly and finally admits that UPnP does not work from the cloud, and throws "WebSockets" against the wall in hopes that it might solve the problem.[249] But as detailed in the attached Technical Analysis, it does not. WebSockets has no meaning absent a defined protocol for information exchange – and proponents have put no thought into security, scaling, servers or anything else to make their proposal work. It proposes an entirely new client server protocol support for UPnP that MVPDs must implement in their networks and an unknown number of servers they must host for purposes of terminating the server side of this

[245] *See* Technical White Paper at 45-46.

[246] CVCC Comments at n.81.

[247] CVCC Technical Appendix at 1-2.

[248] *See*, *e.g.*, *id*. at 4, 5 ("Extensions to support use cases with no MVPD-supplied device in the home (this type of implementation will be referred to as cloud-based.").

[249] *See id*. at 5 ("In order to enable delivery of UPnP events from cloud-based servers, an extension to the UPnP event mechanism will be added utilizing WebSockets.").

network connection.[250] It ignores bandwidth and contention on the access network and latency and performance on the device. It provides no security for the traffic between the user and the server. It does not even fit within the UPnP model it professes to be implementing.[251] It is just one more step in a long line of made-up "solutions" that only serve to highlight that, despite multiple attempts, the proponents of the NPRM have been unable to provide a workable solution.

Rather than "unlocking the box," the proposal will lock in the box and force consumers to use two boxes, and waste electricity needlessly, when an app could provide service with no box at all.[252]

3. The Proposal Still Lacks Device Authentication

Second, the new proposal does nothing to fix the problem that the NPRM does not provide for device authentication. As recounted in the Technical Analysis, in DSTAC the proponents for unbundling used to say that they would build a robust certification regime for "some form of authentication of the device and/or user and/or household."[253] After the complexity of the task was outlined, they abandoned the promise, as has the NPRM.[254] Instead, we are left with a regime of unenforceable self-certifications.

Now, the proponents seek to dignify self-certification by proposing that third parties be allowed to self-provide electronically readable, self-signed certificates posted to a URL. Because there would be no process in place pursuant to which such certificates are validated by a trusted authority, they would be no more reliable than forged drivers' licenses. As a result, MVPDs could not know with certainty whether that certificate is valid – or even if it applies to

[250] Technical Analysis at 15-16.

[251] *See id*.

[252] *See* Taxpayers Protection Alliance Comments at 4; NCTA Comments at 132-135; NRDC Comments at 2.

[253] DSTAC Final Report at 254 (DSTAC WG4 at 119).

[254] Technical Analysis at 14-15.

the device in question. There is no method by which this URL can be validated. A pirate box, hacked device or app would simply substitute the URL for a known compliant device or app in its HTTP requests to masquerade as the compliant device or app. In other contexts, this is called identity theft.[255]

4. The Proposal Makes Device Revocation Even Less Available

Third, proponents have also asked the FCC to further water down any possible revocation to make it even more toothless. MVPDs would be prohibited from shutting off devices known to violate privacy or copyright, and instead would have to continue to feed such devices pending a potentially drawn-out, indeterminate resolution process.[256]

5. The Proposal Still Rejects World Wide Web Consortium Open IP Standards

Fourth, device proponents have always struggled to account in their proposals for modern interactive aspects of MVPD service and service delivery. It has been clear since DSTAC that VOD purchases cannot function on third-party devices without access to a predictable execution environment.[257] The proponents' new proposal tries again. After a year of protesting that HTML5 was unacceptable, now they offer the supposedly unacceptable HTML5 browser – but only to execute a VOD purchase.[258] But as explained in the Technical Analysis, the supposed solution provides no trustworthy or auditable way to handle VOD purchases, or

---

[255] *Id*. at 13.

[256] *See, e.g*., CVCC Comments at 42; Public Knowledge Comments at 51.

[257] *See* Application-Based Service Proponents, Response to Competitive Navigation System Interoperability Additional Material, MB Docket No. 15-64 (Aug. 7, 2015) at 4 ("There is no widget spec that would support PPV/VOD purchasing, VOD playback including LookBack and StartOver, service upgrades, billing, support relating to the MVPDs service, caller ID, sports scores, etc., as claimed by the Device Proposal.").

[258] *See* CVCC Technical Appendix at 3 ("Information required for purchasing either transactional VOD or PPV must be provided by utilizing the *upnp:foreignMetadata* property of the CDS. *This information will either consist of a URL for performing the purchase process via a web browser or use a vendor-specific UPnP action that may require entry of a customer specific PIN code for directly purchasing the content*.") (emphasis added).

account for the wide variety of VOD transactions, because it fails to provide a predictable execution environment.[259]

CVCC's proposal continues to remove all other elements of HTML5. W3C specifies a comprehensive application environment in HTML5, EME, MSE and Web Crypto. But the NPRM and CVCC proposal both reject those open standards developed for IP media streaming, and reject permitting any MVPD application to run on a retail device. For the sole purpose of unbundling a subset of content from MVPD services, the proposed approach forbids MVPDs from using HTTP for its original and main purpose – delivery of full web pages and web apps, the way YouTube, Netflix, Hulu, and all other online video distributors do.

In effect, CVCC proposes a broken version of the web specifically restricted to prevent MVPDs from rendering their service.[260]

6. A New Parity Request Cannot Work With the Three Interfaces

Fifth, CVCC proposes that the Commission add a fourth parity request that "discovery data should include information on the number of simultaneous available streams."[261] This suggestion is erroneously premised on the assumption that the number of simultaneous streams is a fixed number and parity demands that at least this fixed number of streams be available to retail devices. However, in some MVPDs' systems the number of simultaneous streams is not fixed and is actually dynamically determined through proprietary protocols combined with the type (SD, HD, or UHD) and number of content streams being consumed. Unless the retail device implements these proprietary protocols, stream parity cannot work; but the NPRM makes

[259] Technical Analysis at 14-15.

[260] *Id*. at 3, 14-15.

[261] CVCC Comments at 32.

no provision for the use of proprietary protocols for stream management, mandating that only open protocols be used. Consequently, the parity requirement cannot be met.[262]

In truth, there is no "parity" to be found in the NPRM, even with CVCC's additions. Instead, the NPRM would impose significant and unfair advantages on third-party device manufacturers and app developers over their prospective MVPD competitors.

Only MVPDs, but not OVDs, would have their services stripped of competitive features.

The MVPDs that actually pay for the right to distribute the copyrighted content at issue in this proceeding must share that content with third-party device manufacturers and app developers to be repackaged, monetized and presented as their own, but there is no reciprocal obligation that applies to the third parties. This is an unbundling approach that YouTube, Netflix, and Amazon rejected and will not accept for themselves.

Only MVPDs, but not OVDs, would be unable to negotiate content distribution agreements that assure content providers that they could respect the terms for distribution of their content.

Amazon, Google or Apple, could put together a guide that combines their content with MVPDs, but MVPDs could not do the reverse.[263]

By requiring that MVPDs share content with competitive providers via fixed, Commission-mandated protocols, the Commission is effectively ensuring that MVPDs, but not OVDs, lose agile development capabilities and be subjected to the fixed device protocols that

[262] Technical Analysis at 16.

[263] *See* NCTA Comments at 7.

historically slowed cable's innovation.[264] In addition, as Roku has explained, the mere adoption of the rules would create significant multi-year uncertainty that will interfere with innovation.[265]

Only MVPDs, but not OVDs, would be denied the right to use the robust, competitive and dynamic security protections that support rapidly changing new consumer offerings.

"Innovation without permission" is provided for third-party device manufacturers and app developers, but not for MVPDs. CE companies could experiment and innovate. Proponents seek rules that would not only confine MVPD architectures and marketing offers, but constrain all their approaches to "no more than a small number of solutions."

Self-certification is assured for third-party device manufacturers and app developers, despite a long history in technology favoring certification testing. By contrast, MVPD networks, equipment, and implementations would be tested and certified.[266]

The fixed protocols required to achieve the "information flows," and the parity requirements that forbid new cloud-based offerings unless they can also be engineered through the fixed interfaces, would bring cloud-based app development to a halt. "Common Reliance" handicapped innovation and the development of new services and was rejected by all parties in DSTAC consensus recommendations, but "parity" recreates those very burdens. The proposal really is "mutually exclusive" with Comcast delivering service directly to a Roku and other boxless approaches.[267]

---

[264] *See id*. at 145-146.

[265] *See id*. at 7; Roku Comments at 12 ("The proposed rules threaten to put a halt to much of that innovation and growing competition. Roku believes that the proposed rules would create significant uncertainty in the industry, and the reality is that any standard-setting process is likely to be a multi-year process that would lead to disputes within the industry over the direction of any new standards. During the potentially lengthy period of uncertainty, both device makers and video providers would lose the incentive to continue innovating in the manner that is occurring and growing today.").

[266] *See* CVCC Comments at 43.

[267] *See* NCTA Comments at 141-143; *contra* CVCC Comments at 20.

Proponents just keep piling on the market distortions. Comments now seek guaranteed access to an MVPD's cloud DVR, but no MVPD access to a third-party cloud DVR.[268]

And, finally, while MVPDs are subject to the Congressionally-mandated privacy protections of Sections 338(i) and 631, third-party device manufacturers and app developers, who seek to offer a functionally equivalent service, would be exempt from those privacy requirements.[269]

E. Circular References to Unsupported Assertions Do Not Provide Substantive Record Evidence That a Technical Solution Exists

The record in this proceeding fails to establish that the technology proposals advanced in the NPRM or by its proponents will securely deliver MVPD service to third party retail devices. Rather than treating copyright, security, theft, bandwidth, or anything else seriously and deal with serious solutions, proponents have relied on baseless talking points, fallacies, and demonstrably defective technology claims which, however often repeated, still provide no basis for adopting the rules. They have also manufactured the *appearance* of record evidence through a series of circular references to their own unsubstantiated claims. Any rule premised on such "record evidence" would be arbitrary and capricious.

For example, the proponents' October 2015 *ex parte* discussed above claimed to describe "an approach … that would allow for competitive navigation devices to operate on MVPD systems on a uniform basis."[270] NCTA effectively refuted those claims, as have others.[271]

---

[268] *See* TiVo Comments at 14.

[269] *See* Legal White Paper at 37-40; *supra* at 9-10.

[270] Public Knowledge Oct. 20, 2015 *Ex Parte* at 1.

[271] *See* NCTA DSTAC Reply Comments at 26-36; Technical Analysis at 7-11; Letter from MPAA, NCTA, ITTA – The Voice of Mid-Size Communications Companies, NTCA – The Rural Broadband Association, ACA, ARRIS Group, Inc., AT&T/DIRECTV, Bright House Networks, LLC, Cable Television Laboratories, Inc. (CableLabs), CenturyTel Broadband Services, LLC d/b/a CenturyLink, Charter Communications, Inc., Cisco Systems, Inc., Comcast Cable Communications, Inc., Cox Communications, Inc., DISH Network LLC, EchoStar Technologies LLC, Time Warner Cable Inc. to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Nov. 5, 2015); Letter

Nevertheless, the NPRM cited to that submission to support its claim that a working solution apparently exists, asserting that "the specifications necessary to provide these information flows appear to exist today."[272] Completing this unvirtuous circle, CVCC in its Comments *on the NPRM* merely refers back to the NPRM's *citation of its own Comments* – but offers no substantive, technical support for these claims because none exists. There is a big difference between assembling a legitimate record on which to base an agency rule and relying instead on unsubstantiated talking points that have been reiterated in the echo chamber of this proceeding to purport to provide that record. As has been said in a related context, merely repeating slogans does not provide solutions.

As another example, proponents have conflated the top level user interface, menu structure, look and feel that distinguishes an Apple tablet, an Android tablet, a Roku and a Samsung Smart TV with the user interface that each app provider uses to provide and distinguish its own service. During the DSTAC process proponents argued that consumers lack choice for navigation devices because competitive providers must be able to substitute a service provider's user interface and repurpose its programming. Despite repeated challenges to produce any supporting evidence, proponents produced none. The DSTAC Report found that "no evidence whatsoever has been presented to the DSTAC to indicate that [a retail device's own] guide is the recipe for success of competitive navigation devices, or that customers want the device maker to block available MVPD services."[273] NCTA has demonstrated that competing navigation device

---

from Paul Glist, Counsel for NCTA (joined by Comcast, Charter, Cox, Cablevision, CableLabs, and MPAA) to Marlene H. Dortch, Secretary, FCC, MB Docket No. 15-64 (Jan. 13, 2016).

[272] NPRM at ¶ 35.

[273] DSTAC Final Report at 283 (DSTAC WG4 at 148).

UIs pervade the marketplace without replacing the video provider's guide or experience.[274] Nevertheless, the NPRM repeats the claims that replacing the video provider's guide is essential for success – and in turn, CVCC cites back to that NPRM in the echo chamber of this fallacy.[275]

As a third example, proponents similarly argued during DSTAC that DTCP constitutes a "standard." NCTA subsequently explained that DTCP is a propriety security solution, not a standard within the video-distribution marketplace, and has documented that the actual video market overwhelmingly relies upon a combination of agreements, DRMs and apps (i.e., trust infrastructures) to secure service. Notwithstanding this real-world evidence, the NPRM repeats the claim that DTCP is a "standard." CVCC completes the feedback loop in its Comments.[276]

Circular references to unsubstantiated claims are no evidence at all, and reliance on them would be arbitrary and capricious.

F. The Proposal Continues to Suffer from Unfixable Failings in its Foundation

As the Technical Analysis explains, all of the proposals from CVCC, including that contained in the NPRM, share three fundamental common failings:

- Broken Chain of Trust: they all include multiple security failings that weaken MVPD security and the associated trust infrastructure.
- New Leased Device Requirement: they all require installation of an MVPD-specific device in every MVPD home due to the failure for the proposal to technically deliver a "cloud-based" approach.
- Broadcast-only: they all rely on a three-stream architecture that reduces interactive cable services into broadcast-only (one-way) services, removing the necessary support for

[274] *See id*. at 283-284 (DSTAC WG4 at 148-149); NCTA Comments at 22-30; John Solit, *An Interface by Any Other Name*, NCTA PLATFORM BLOG (May 4, 2015), https://www.ncta.com/platform/technology-devices/an-interface-by-any-other-name/.

[275] NPRM at ¶ 27 ("MVPDs and unaffiliated vendors must be able to differentiate themselves in order to effectively compete based on the user interface and complementary features they offer users"); TiVo Comments at 14-15 (citing NPRM, but providing no evidence).

[276] NPRM at ¶ 55; CVCC Comments at 38-40.

essential aspects of MVPD service such as Video-on-Demand (VoD), user identification, and device registration, and other interactive elements.[277]

"The history of these proposals does not reflect thoughtful development and refinement, nor the competitive demands of the MVPD service offerings today. It instead reflects haphazard efforts to assemble a series of unworkable proposals that never address the underlying set of problems that makes the proposals unworkable. If any of the device proposals, including the conceptual one advanced in the NPRM, were technically feasible, it would have been possible for their proponents to put forth a consistent and stable proposal."[278] The Technical Analysis concludes: "The proponents' inability to address the fundamental problems created by 'unbundling,' notwithstanding the intense work undertaken since the beginning of the DSTAC process in January 2015, indicates that the 'Competitive Navigation' proposal is technically infeasible. The root problem is that all of these proposals have abandoned the applications and trust infrastructure that is a foundational requirement for modern MVPD service."[279]

G. No Quick Technical Solution Exists

The NPRM and CVCC claim that all of the outstanding issues and intractable problems that have been identified with this unfixable proposal can be addressed in an incredibly short amount of time. But there is no basis for this claim. Industry participants have provided specific warnings, and numerous examples of similarly scoped undertakings that demonstrate that none of this can be accomplished in the two years that the proposal would provide.

As DLNA pointed out in its Comments, "it has substantial experience in projects of this complexity, demonstrating that much longer than one year is required for a project of this

[277] Technical Analysis at 16.

[278] *Id*. at 4.

[279] *Id*. at 17.

magnitude. Even the average time for DLNA projects is 36 months +/- 12 months for end-to-end projects including project definition, guideline creation, test program creation, plugfests, certification program creation and validation."[280] VidiPath took much longer. CableCARD took 6 years, HTML5 media streaming standards took 11 years, and 1394 took 9 years. It is arbitrary to expect full standardization and deployment of a solution in 2 years.[281]

IV. THE PROPONENTS FAIL TO DEMONSTRATE THAT THE PROPOSED RULES ARE A LAWFUL IMPLEMENTATION OF SECTION 629

As detailed in NCTA's Comments and Legal White Paper, Section 629 was adopted in a different world where cable served over 90% of multichannel consumers, and consumers had little choice but to lease a set-top box from cable to receive cable programming. The purpose of Section 629 was to give consumers the option to purchase a set-top box at Circuit City on which to receive multichannel services and other services *"offered"* and *"provided"* by MVPDs. The FCC has repeatedly and consistently ruled that Section 629 authorizes the Commission only to assure a market for retail equipment that receives *MVPD services*, not to receive some selected parts or derivative service that a CE manufacturer may wish its product to provide.[282] It has specifically ruled that a third-party guide is *not* a navigation device.[283]

---

[280] Digital Living Network Alliance (DLNA) Comments at 2.

[281] As explained in DSTAC and in NCTA Comments, HTML5 with streaming media extensions is an open W3C standard designed and deployed to present each publisher's content through a web page designed and tailored to the content by the publisher, not a third party's user interface. *See* NCTA Comments at 28; DSTAC Final Report at 81-91, 230-34 (DSTAC WG3 at 23-33; DSTAC WG4 at 95-99).

[282] *See Gemstar Int'l Group, Ltd.*, Memorandum Opinion and Order, CSR 5528-Z; CSR 5698-Z, 16 FCC Rcd 21531, 21542, ¶ 31 (2001) ("*Gemstar*") ("Section 629 is intended to assure the competitive availability of *equipment*, including '*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.' The Commission has not found that the right to attach consumer electronics equipment to a cable system can be expanded to include the obligation by cable operators to carry any service that is used by such equipment, nor is the legislative history supportive of such a requirement. Indeed, the scope of Section 629 apparently was 'narrowed to include only equipment used to access services provided by multichannel video programming distributors.'" (citing S. Conf. Rep. No 104-230 at 181 (1996), footnotes omitted)). *Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices*, Report and Order, CS Docket No. 97-80, 13 FCC Rcd 14775 ¶¶ 1, 7 (1998) ("[W]e adopt rules to address the mandate expressed in Section 629 of the Communications Act to ensure the commercial availability of 'navigation devices,'

Nothing in Section 629 supports the unbundling of cable to promote different services, guides, user interfaces, or video providers, and many provisions in Title VI forbid it. Trying to extract that expansive authority from a clearly limited statute is particularly unsupportable in today's world where ninety-nine percent of homes have access to at least three MVPDs, thirty-five percent have access to four MVPDs, there are more OVD subscriptions to Netflix, Amazon, and Hulu alone than to all MVPDs combined, and MVPDs make their apps available on more than 460 million customer-owned devices in the United States —more than twice the number of set-top boxes currently in use.

Such an expansive view of Commission authority also violates well-established Constitutional rights. The First Amendment forbids interfering with MVPDs' rights to control the selection and presentation of their services, compelling them to alter the presentation of their services, and precluding them from reaching their subscribers with their own messages. The NPRM's proposal would also violate exclusive rights granted program providers, MVPDs, and guide vendors under the Copyright Act and Lanham Act and circumvent technological protection measures protected by the Digital Millennium Copyright Act.

The NPRM's proponents offer little analysis in support of the legality of the FCC's proposal. Apparently, their view is that the combination of Section 629, STELAR and the Commission's successful defense of its integration ban (but not its plug and play rules) in court means that it can now adopt any rules it claims would promote a retail market for set-top boxes. This is incorrect, not only because the D.C. Circuit has specifically warned against such

---

the equipment used to access video programming and other services from multichannel video programming systems. The purpose of Section 629 and the rules we adopt is to expand opportunities to purchase this equipment from sources other than the service provider."). *Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices*, Order on Reconsideration, CS Docket No. 97-80, 14 FCC Rcd 7596, 7601 ¶ 12 (1999) ("The objective of Section 629 is to open new competitive outlets for devices that in the past have tended to be exclusively available from or under the control of service suppliers.").

[283] *See Gemstar* at ¶ 31.

"unbridled" constructions of Section 629, but also because the proposed rules, by their terms, fall far outside the language and purpose of the statute. The Commission must adequately justify its proposed rules under the framework of the authority delegated to it by Congress in the Communications Act, which, as explained in the Legal White Paper attached to NCTA's comments, the Commission has failed to do. As demonstrated below, the recent legal arguments from NPRM proponents fare no better.

A. STELAR Does Not Grant Any New Authority to the Commission

CVCC claims that the NPRM is a "natural continuation" of STELAR,[284] but STELAR did not grant any substantive rulemaking authority to the Commission; it only placed an obligation on the Chairman to convene DSTAC to deliver a report on downloadable security to the Commission, an obligation that has now been discharged.[285] But even if STELAR were a new grant of authority, the Commission would then be obligated to comply with its terms when relying on it for authority in this proceeding. As we and others have demonstrated, the NPRM proposal is *in conflict with* STELAR's call for any solution to be "technology and platform neutral,"[286] because the proposed rules would create significant new disparities in the video marketplace by burdening MVPDs with technical mandates, costs and other requirements and

---

[284] CVCC Comments at 11 (referencing STELA Reauthorization Act of 2014, H.R. 5728, 113th Cong., § 106 (2014) ("STELAR")).

[285] *See Motion Picture Ass'n of Am., Inc. v. F.C.C.*, 309 F.3d 796, 807 (D.C. Cir. 2002) ("Congress authorized and ordered the Commission to *produce a report* – nothing more, nothing less . . . . Once the Commission completed the task of preparing the report . . ., its delegated authority on the subject ended."). As explained in the NCTA Legal White Paper at 4, Congress did not adopt an expansive FCC rulemaking mandate in the STELAR Act, although one such amendment was proffered and then withdrawn by its sponsor for lack of support. *See* Amendment of Sen. Edward Markey to S. 2799 (2014) ("Markey Amendment") (proposing that the FCC adopt rules for a "methodology for access to a system's programming features, functions, and services"); *see also* DSTAC Final Report at 284 n.54 (DSTAC WG4 at 149 n.54) (noting that the Markey Amendment "would have assigned DSTAC an expansive mission to develop a new technology mandate for the FCC to adopt by rule" but that it was withdrawn by its sponsor for lack of support and thus did not become part of the law).

[286] STELAR § 106(d)(1) (2014). CFA also agrees that any rules should be "technology-neutral, product-neutral." *See* CFA Comments at 7.

exempting OVDs.[287] The proposal is also contrary to STELAR's command that any proposed solution be "not unduly burdensome," because the proposed rules would require MVPDs to redesign their networks and either deploy cloud services supporting the three information flows or to develop, test, and deploy an FCC mandated device for the home.[288]

B. The Fact that Equipment Can Include Embedded Software Does Not Make All Stand-Alone Software "Equipment"

The NPRM's proponents contend that the Commission's authority extends to all hardware and software associated with the viewing of multichannel video programming. For example, TiVo asserts "that the Commission's authority extends to both hardware and software means used by consumers to access multichannel video programming and thus extends to assuring a competitive retail market for "apps" used to access MVPD content."[289] This interpretation cannot be reconciled with the plain meaning of the term "equipment," the intended meaning of which must be informed by the words surrounding it in the statute, all of which refer to hardware: "converter boxes, interactive communications equipment, and other equipment."[290] While of course it is true that navigation device hardware typically includes embedded software that might reasonably be deemed part of the device, that fact does not "magically transform" the entire universe of other unrelated software applications into navigation device equipment.[291]

---

[287] *See, e.g.,* NCTA Comments at 147 (noting that "the proposed rules would enable a select few companies to help themselves to the content of MVPDs while fiercely defending their own brands and offerings from competitors"); AT&T Comments at 37 ("Netflix, YouTube, Amazon, and any other OVD can update and enhance their services simply by upgrading their app, which can be distributed to all users instantaneously… if an MVPD wishes to update its service, it will first have to ensure that the upgrade will comply with the parity requirements."); Cox Comments at 5 (noting "the NPRM's departure from any semblance of regulatory parity. If there were such parity, services like Netflix and Amazon, devices like Apple TV, and the envisioned Google devices or applications would be similarly encumbered by obligations to unbundle their services for other devices or applications to package as their own.").

[288] *See* Technical White Paper at 45.

[289] *See* TiVo Comments at 12; *see also* CVCC Comments at 8; Public Knowledge Comments at 5-6.

[290] 47 U.S.C. § 549(a). *See, e.g., Yates v. United States*, 135 S. Ct. 1074, 1085 (2015) (a statutory term must be read in light of "the company it keeps").

[291] *See* AT&T Comments at 70-71.

The Commission no doubt may try to make a case that stand-alone software that performs the same functions as navigation hardware did in the past *should be* considered a navigation device in order to effectuate Congressional intent notwithstanding changes in technology. The first problem with that argument is that honoring Congressional intent requires limiting Section 629 to those navigation devices that are used to access an MVPD's services as offered and provided by the MVPD, as Congress set forth in the statute.[292] The third-party stand-alone apps that the NPRM envisions ingesting the information flows would present different, reconstituted services. Moreover, there has been no proposal advanced that can meet the specific commands of Section 629(b) not to jeopardize security, of Section 624(f) not to "impose requirements regarding the provision or content of cable services, except as expressly provided in [Title VI],"or of Section 621(c) not to impose any type of common carrier regulation on a cable operator's provision of cable services.[293] The Commission cannot ignore the plain meaning of the word equipment in order to effectuate a supposed Congressional end that Congress plainly did not intend. Therefore, standalone software such as apps should not be deemed "equipment" for purposes of this proceeding.

C. The NPRM Vests Standards Bodies With Too Much Authority

In Section 629, Congress directed the Commission to "consult with appropriate industry standard-setting organizations" in adopting any regulations.[294] Accordingly, the FCC should be considering the conclusions of worldwide standards bodies that have embraced apps and related standards as part of its own rulemaking process. But instead, the proposed rules would impose a radical technology mandate for MVPDs to provide three disaggregated information flows and

[292] *See* NCTA Comments at 162-164; Legal White Paper at 13-30.

[293] Legal White Paper at 26-29, 31-36.

[294] 47 U.S.C. § 549(a).

punt the critical details to private standard-setting bodies to legislate without accountability, with the standard automatically adopted as effective national law. Such an approach is not only inconsistent with Section 629 but runs afoul of constitutional limitations on the power of federal agencies to delegate away their authority to private, unaccountable and inherently biased bodies.

Sensing the opportunity to impose their own self-serving demands through a standards body with no legal or political accountability, one NPRM proponent asks that standards bodies require all intellectual property rights to be licensed on reasonable and non-discriminatory (RAND) terms[295] – contrary to the FCC's decision in analogous cases not to specify the IP licensing model for intellectual property involved in content protection.[296] Another calls for "a nonaggression covenant through which licensors promise not to use anti-circumvention law to interfere with security research"[297] – an approach that was rejected by W3C.

To assure dominance over the process, NPRM proponents have also made many requests to "stack" the vote of a supposedly open standards body. INCOMPAS, for example, argues that the standards body should let all comers vote regardless of participation and that voting be controlled so that the standards body is "completely independent of MVPD and programmer

[295] TiVo Comments at 22.

[296] In prior orders, the FCC has specifically declined to specify any particular technology licensing model – RAND, non-assert, or otherwise – that is appropriate for content protection. *Basic Service Tier Encryption*, Report and Order, MB Docket No. 11-169, 27 FCC Rcd 12786 ¶ 24 (2012) ("Basic Service Tier Encryption Order") ("In adopting this 'good faith' licensing requirement, we intentionally do not specify any particular technology or technology licensing model (e.g., we do not require or specify 'fair, reasonable, and non-discriminatory' licensing, as that term has been interpreted in other contexts, as urged by Boxee and CEA)."); *Digital Output Protection Technology and Recording Method Certifications*, Order, MB Docket Nos. 04-55 to 04-66; 04-68, 19 FCC Rcd 15876 at ¶ 91 (2004) ("With respect to the potential for certain license terms to serve as ancillary restraints on competition and technical innovation, the record in this proceeding does not support the Commission's adoption of one approach to intellectual property licensing over another.").

[297] *See* Electronic Frontier Foundation (EFF) Comments at 10.

control"[298] – approaches that directly contradict ANSI standards for how open standards are reached through consensus among all materially affected and interested parties.[299]

The NPRM would improperly delegate to non-governmental standards bodies the ability to establish binding legal requirements. This proposed standards process is designed to vest competitors with regulatory authority over MVPDs.[300] Such delegation of regulatory power "undertakes an intolerable and unconstitutional interference with personal liberty and private property."[301] As discussed in the Legal White Paper included with NCTA's Comments, the NPRM "attempts an end-run around the Commission's lack of statutory authority to dictate binding standards for the industry by relying on private 'open standards bodies' to set binding technical standards for accessing all MVPDs' content."[302] Even supporters of the NPRM's general approach are concerned about any delegation of authority to standards bodies that would allow parties to pursue self-interested agendas.[303]

For all of these reasons, the NPRM's proposed framework for involving open standards bodies in its new unbundling regime is arbitrary, unworkable, and unlawful.

---

[298] *See* INCOMPAS Comments at 18-19.

[299] *See, e.g.*, American National Standards Institute (ANSI), Critical Issue Paper: Current Attempts to Change Established Definition of "Open" Standards (May 2005), available at https://share.ansi.org/shared%20documents/Standards%20Activities/Critical%20Issues/Open%20Standards/CIP-OpenStandards.pdf (defining an "open standard" as the product of a "process that has certain important features," including "consensus by a group or 'consensus body' that includes representatives from materially affected and interested parties"); *see also* ANSI, Frequently Asked Questions, ANSI.org (last visited May 13, 2016), http://www.ansi.org/about_ansi/faqs/faqs.aspx?menuid=1 ("American National Standards are voluntary and serve U.S. interests well because all materially affected stakeholders have the opportunity to work together to create them.").

[300] *See Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936) (invalidating a statute that empowered majority coal producers to regulate minority coal producers); *Ass'n of Am. Railroads v. U.S. Dep't of Transp.*, No. 12-5204, 2016 WL 1720357, at *12, 17 (D.C. Cir. Apr. 29, 2016) (holding that a federal statute violated the Due Process Clause because it delegated Amtrak regulatory control over its competitors).

[301] *See Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936).

[302] *See* Legal White Paper at 66-67; ACA Comments at 74-76.

[303] *See* Greenlining Institute Comments at 6-9.

V. THE PROPONENTS FAILED TO DEMONSTRATE THAT ADDITIONAL PROPOSED REGULATIONS ARE NECESSARY TO PROTECT CONSUMERS

A. No Party Has Offered Any Specific Evidence Demonstrating an Actual Need for Re-Adoption of the Outdated CableCARD Support and Reporting Rules

The NPRM asks whether the CableCARD support rules should be "retained."[304] As noted in NCTA's comments, these rules were vacated by *EchoStar v. FCC*.[305] The court vacated the original plug-and-play rules, including Rule 15.123 which defined unidirectional digital cable-ready products ("UDCPs") and Rule 76.640 which defined support for UDCPs. The 2010 CableCARD support rules referenced by the NPRM were expressly applicable only to MVPDs "subject to the requirements of [the now vacated] Section 76.640,"[306] so while the rules may still exist, technically they apply to no one. Nonetheless, in its recent order approving the Charter/Time Warner Cable/Bright House Networks merger, the Commission stated that *EchoStar* "did not … vacate or even address the CableCARD customer support rules that the Commission adopted in 2010"[307] – and yet, doubtful of that legal assertion, it imposed the substance of the rules as a merger condition because no rule is in force.

The parties arguing for "retention" or re-adoption of these rules have not offered any evidence that any of those rules are relevant and necessary today. TiVo expresses a general concern that cable companies will cease supplying and supporting CableCARDs to subscribers using retail devices,[308] but no party details any *actual* ongoing problems with CableCARD

---

[304] NPRM at ¶ 87.

[305] NCTA Comments at 173 (citing *EchoStar Satellite L.L.C. v. FCC*, 704 F.3d 992 (D.C. Cir. 2013)).

[306] *Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices et al.*, Order on Reconsideration, CS Docket No. 97-80, PP Docket No. 00-67, CSR-7902-Z, FCC 11-7, 26 FCC Rcd 791, Appendix (2011).

[307] *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership For Consent to Assign or Transfer Control of Licenses and Authorizations*, Memorandum Opinion and Order, MB Docket No. 15-149, FCC 16-59 at ¶ 249 (rel. May 10, 2016). This order cannot lawfully be read as amending the Commission's rules or adopting a new rule.

[308] *See* TiVo Comments at 35.

support procedures that would justify the resurrection of the specific CableCARD support rules. None of the commenters has provided evidence that support for CableCARDs by MVPDs has "in fact gotten worse in recent years."[309] Cablevision has utilized SmartCards and then downloadable security for its own set-top boxes for over a decade with no measurable reduction in support for CableCARDs for retail devices. Likewise, there is no demonstrable reduction in industry-wide support for CableCARDs since *EchoStar*. As NCTA Comments documented, years of cable industry support for CableCARDs has continued, with TiVo applauding Comcast for "continued commitment to CableCARD provisioning and support" and going well beyond any requirements from the vacated plug and play rules.[310]

As the Commission noted, cable operators are still obligated to provide separable security under Rule 76.1204(a)(1).[311] And, as a practical matter, there are more than 55 million CableCARDs currently deployed in cable-provided devices.[312] Cable operators have strong business incentives to ensure that CableCARDs continue to function properly. Given this reality, the re-adoption of the CableCARD support rules is unnecessary.

Only one party, CVCC, commented in favor of retaining the CableCARD quarterly reporting requirements, and did so almost as an afterthought, stating only that "[t]he Commission should retain its CableCARD support and reporting rules," with no ensuing explanation of any

---

[309] *Id*. at 32.

[310] NCTA Comments, Appendix D, Timeline of Cable Industry Support for CableCARDs at 5 (2014: "TiVo tells the FCC that 'Comcast has again partnered with TiVo to work on a two-way non-CableCARD security solution that will enable retail devices to access the full Comcast lineup of linear and VOD programming, whether QAM- or IP-delivered.'" 2016: "Comcast working towards offering a self-service tool for CableCARD activation, an option to direct-ship CableCARDs for self-installation, and a single support line for all CableCARD activation, support and billing questions.").

[311] *See* NPRM at ¶ 90 (noting that the separated security requirement "remains in effect").

[312] *See* Letter from Neal M. Goldberg, Vice President and General Counsel, NCTA to Marlene H. Dortch, Secretary, FCC, CS Docket No. 97-80 (Apr. 27, 2016) (reporting that the "nine [largest cable] companies have more than 55,000,000 operator-supplied set-top boxes with CableCARDs currently deployed").

benefit of the reports.[313] As we said in our initial Comments, no ongoing purpose is served by these reports and the requirement – which is not embodied in an FCC rule – should be eliminated.

B. Reimposition of the Encoding Rules Is Unnecessary

TiVo's comments also inject a request not raised by the NPRM: it asks the Commission to readopt and apply its vacated encoding rules to all MVPDs.[314] These are the very rules vacated three years ago by the D.C. Circuit as beyond the FCC's jurisdiction. As was the case with a 2013 TiVo petition raising the same issue, TiVo provides no evidence whatsoever that MVPDs have been arbitrarily encoding content to disadvantage retail devices, which was the animating concern and basis for adopting encoding rules in the first place. Nor has TiVo supported its naked assertion that an "infinite number of difficult to determine and ever-changing copy protection levels across all MVPDs" has arisen since *EchoStar*.[315]

But imposing such rules on MVPDs would have a serious distorting effect in today's marketplace. Online video providers would not be bound by the encoding rules, and Netflix's recent proposal to stream a *Relativity* movie to homes even before theatrical release[316] illustrates what a distorting effect adoption of such rules could have on the video marketplace. A content provider that wanted to offer secure streaming only of early release content could reach any

[313] CVCC Comments at 48.

[314] *See* TiVo Comments at 19-21.

[315] *Id*. at 21.

[316] Tom Corrigan and Erich Schwartzel, *Netflix Plan to Stream Relativity Films Threatens Studio's Comeback*, WALL ST. J. (May 9, 2016), http://www.wsj.com/articles/netflix-plan-to-stream-relativity-films-threatens-studios-comeback-1462848259 ("Netflix Inc. is threatening to stream two films produced by Relativity Media LLC before their debut in theaters….").

agreement it wished with TiVo or an online video provider. But an MVPD would need to wait years for a waiver of selectable output restrictions.[317]

TiVo claims that new encoding rules would "serve to limit consumer confusion and help establish consumer expectations regarding how different types of programming and services can be used."[318] But the only consumer confusion at issue is that which would arise under TiVo's scheme as consumers would struggle with understanding why streaming only services cannot be copied when cable services can be.[319]

C. There Is No Need to Turn Back the Clock to Rate Regulation

No comments demonstrate a legal basis or need for adoption of the so-called "billing transparency" rule. As explained in NCTA's comments, Congress made clear that concerns over equipment subsidies are moot when service markets are competitive and all MVPD are now subject to or presumptively subject to effective competition nationwide. As an economic matter, set-top boxes may be considered complements to the multichannel services they support, and there is no evidence that set-top box pricing – whether it is zero for AT&T or $11.99 for Verizon – has any material effect on subscribership. The comments reveal no legal support for the proposal, but only the inconsistent claims that MVPDs charge too much for set-top boxes[320] and should be precluded from charging too little.[321]

---

[317] The Commission took two years to grant a waiver of the encoding rules for MVPDs to offer early-release theatrical content. *Motion Picture Association of America; Petition for Expedited Special Relief; Petition for Waiver of the Commission's Prohibition on the Use of Selectable Output Control (47 C.F.R. § 76.1903)*, Memorandum Opinion and Order, CSR-7947-Z; MB Docket No. 08-82, 25 FCC Rcd 4799 (MB 2010). We discuss in NCTA Comments at 106-109 that it is a net loss to competition and consumers for service providers to be confined to one size fits all ways of offering their services.

[318] TiVo Comments at 21.

[319] Some sites explain why this is so. *See, e.g.*, Tablo, *Tablo FAQs – Can I Record Streaming Services Like Sling TV or Netflix with Tablo?*, TABLO BLOG (June 16, 2015), https://www.tablotv.com/blog/can-i-record-sling-tv-netflix-tablo/.

[320] Public Knowledge Comments at 15. CVCC argues that MVPDs are subsidizing their services via leased navigation device fees. *See* CVCC Comments at 47. INCOMPAS adds even more extravagant hyperbole –

Although touted as a pro-consumer argument, the "billing transparency" proposal would instead have the anti-consumer effect of blocking MVPDs from offering free or deeply discounted set-top boxes. As NCTA explained in its opening comments, free navigation devices have been provided by MVPDs in numerous circumstances with FCC endorsement.[322] Set-top boxes continue to be offered for free or at heavily discounted prices today, as reported to – but not, in turn, reported by – the Markey/Blumenthal survey.[323] Finally, no party filed comments in support of the proposals set forth by Montgomery County for the Commission to impose a wide range of new rate regulations on MVPDs. Accordingly, there is no basis in the record to adopt its proposals, which conflict with the recent Commission decision that cable operators are presumptively subject to effective competition and that such operators should not be subject to rate regulation.[324]

CONCLUSION

The record in this proceeding is clear and the record evidence is overwhelmingly against the FCC's preferred proposal in the NPRM. It is proponents of that FCC tech mandate who offer only empty slogans, not substantive solutions, for bringing MVPD services to retail devices. By

---

claiming that such charges continue "even after the cable systems have recovered the cost," INCOMPAS Comments at 6, when, as NCTA has explained, since 1993 the FCC established rate regulation rules for cable set-top box rents provide that "subscriber charges for such equipment shall not exceed charges based on actual costs" in accordance with the requirements set forth in FCC regulations. NCTA Comments at 138-141.

[321] *See, e.g.,* TiVo Comments at 31 (advocating a prohibition on cross-subsidization, to prevent disadvantages to competitive devices via low MVPD pricing); Public Knowledge Comments at 52-53 (proposing that the Commission should "prevent unfair cross-subsidization," which would "put competitive apps and devices at a disadvantage"). The Commission has looked with disfavor on predatory pricing claims of this sort in the past. *See Earthlink, Inc. v. SBC Communications, Inc., et al.*, Memorandum Opinion and Order, EB Docket No. 14-207 (May 4, 2016); *Joint Application by SBC Communications, Inc., et al., for Provision of In-Region, InterLATA Services in Kansas and Oklahoma*, Order on Remand, 18 FCC Rcd. 24474 (2003). And the cognizability of such claims is being reduced with each passing Supreme Court decision. *See, e.g., Pacific Bell Telephone v. Linkline Communications, Inc.*, 555 U.S. 438 (2009).

[322] *See* NCTA Comments at 169-70.

[323] *See id.* at 170, 138-39.

[324] *See id.* at n.410.

contrast, MVPDs' apps already make their services available to consumers on retail devices, and enjoy widespread support from consumers, CE manufacturers and industry leaders around the world – while preserving and promoting independent innovation in networks, services, and devices and preserving statutory and regulatory consumer protections in a manner consistent with the Communications Act and the Constitution. The only way to serve the fundamental goal of Section 629 is to stop pursuing the NPRM's unbundling approach and support the apps-based approach included in the DSTAC Report.

Respectfully submitted,

/s/ Neal M. Goldberg

Rick Chessen
Neal M. Goldberg
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

Paul Glist
Paul Hudson
Davis Wright Tremaine LLP
1919 Pennsylvania Avenue N.W. – Suite 800
Washington, D.C. 20006-3401

May 23, 2016

APPENDICES

APPENDIX A – A TECHNICAL ANALYSIS OF THE MULTIPLE "COMPETITIVE NAVIGATION" PROPOSALS

Ralph W. Brown

APPENDIX B – SELECTION OF PROGRAMMER APPS

APPENDIX A

A TECHNICAL ANALYSIS OF THE MULTIPLE "COMPETITIVE NAVIGATION" PROPOSALS

Ralph W. Brown

A Technical Analysis of the Multiple "Competitive Navigation" Proposals

Ralph W. Brown

CableLabs

May 23, 2016

Ralph W. Brown
Chief Technology Officer
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027-9750

Table of Contents

Executive Summary 3
I. Introduction 4
II. Proposal 1: DSTAC WG Report – August 28, 2015 5
III. Proposal 2: Public Knowledge Ex Parte Filing - October 20, 2015 7
A. Elimination of X.509 Certificates 8
B. Change in Discovery Protocol and Elimination of PlayReady DRM 8
C. Elimination of MMI "Widgets" Concept 10
D. Other Technical Issues in the Public Knowledge Ex Parte Filing 11
IV. Proposal 3: Technical Appendix to CVCC Comments - April 22, 2016 11
A. Numerous Security Failings 12
B. Inadequate Support for User Interaction 14
C. Requirement for an MVPD Specific Device in the Home 15
D. Other Technical Issues in the Technical Appendix to CVCC Comments 16
Conclusion 16

A Technical Analysis of the Multiple "Competitive Navigation" Technical Proposals

Ralph W. Brown

CableLabs

May 23, 2016

EXECUTIVE SUMMARY

While proponents of an unbundling approach continue to change their proposal with each new filing, they still fail to provide a technically feasible approach to satisfy Section 629. This technical report provides an analysis of the three different proposals[1] and traces the efforts of the proponents to address the inherent technical problems of their proposals. This analysis demonstrates that none of these three proposals actually address the underlying technical issues. They instead demonstrate a haphazard approach, switching the standards used, flip-flopping on a number of critical issues that ultimately erode security and failing to deliver on the principal architectural component of a "Cloud-based Virtual Headend."

The device proponents have made three substantially different proposals over the past nine months: one in the DSTAC Report, one in a subsequent Ex Parte filing, and a third more recently in comments on the FCC's NPRM in MB Docket 16-42. While each of these proposals individually has numerous major technical issues and often relies on non-existent or yet-to-be invented standards, none of them actually deliver a solution that could be implemented using the information provided in their proposals. The proponents claim that all of these proposals leverage standards broadly adopted by all MVPDs and that any technical issues with them are minor and could be easily resolved with simple "tweaks" to these existing standards. This technical analysis of the three proposals clearly refutes these assertions.

The changes in each subsequent proposal are neither minor, nor are they simple "tweaks;" rather, they represent major shifts in how they propose their solution fundamentally works. One example of these major shifts is first proposing a very vague definition of optional user-interface "widgets," then proposing no user interaction capability at all, and then proposing restricted web

[1] The "competitive navigation" or "device" proposal was very similar to a proposal the FCC considered in 2010, called "AllVid," that would have forced all MVPDs to establish a common interface for connection to televisions, DVRs, and other smart video devices. The FCC ultimately took no action on the proposal. Proponents of the similar approach included in DSTAC originally called themselves the AllVid Alliance.

browser functionality in the retail device that is limited only to specific user interaction functions. Another example has occurred on the security front, where the proponents shifted from a reliance on DTCP with an optional DRM, then to DTCP alone, then to DTCP with two specific DRMs and a mandatory key exchange. A third example is in certification, where the proponents shifted from a reliance on an abstract device X.509 certificate scheme for device authentication, to optional device authentication, to a device authentication mechanism that is trivially spoofed and therefore ineffectual. Finally, the proponents have offered three different proposed "Cloud-Based Virtual Headend" architectures that attempt to extend home networking discovery protocols to be used over an entire MVPD's subscriber base, but none of them technically work.

All of the proposals share three fundamental common failings:

1. Broken Chain of Trust: they all include multiple security failings that weaken MVPD security and the associated trust infrastructure.
2. New Leased Device Requirement: they all require installation of an MVPD-specific device in the home due to the failure for the proposal to technically deliver a "cloud-based" approach.
3. Broadcast-only: they all rely on a three-stream architecture that reduces interactive cable services into broadcast-only (one-way) services, removing the necessary support for essential aspects of MVPD service such as Video-on-Demand (VoD), user identification, device registration, and other interactive elements.

The history of these proposals does not reflect thoughtful development and refinement, nor the competitive demands of the MVPD service offerings today. It instead reflects haphazard efforts to assemble a series of unworkable proposals that never address the underlying set of problems that makes the proposals unworkable. If any of the device proposals, including the conceptual one advanced in the NPRM, were technically feasible, it would have been possible for their proponents to put forth a consistent and stable proposal. The proponents' inability to address the fundamental problems created by "unbundling," notwithstanding the intense work undertaken since the beginning of the DSTAC process in January 2015, indicates that the "competitive navigation" proposal is technically infeasible.

I. INTRODUCTION

In order to consider the CVCC's most recent Technical Proposal in context, it is worthwhile to review the various alternative unbundling approaches the device proponents have put forth since the beginning of the DSTAC process in January 2015.

The proponents have advanced three different proposals:

- one in the DSTAC Report;[2]

[2] The DSTAC Report actually contained two distinct and incompatible proposals from the device proponents: one proposed exclusive use of DTCP for security (in WG3), and the other proposed use of Microsoft PlayReady (in

- a second in an October 20, 2015 ex parte filing by Public Knowledge;[3] and
- a third in an April 22, 2016 Technical Attachment filed by CVCC in FCC MB Docket 16-42.[4]

While the proponents continue to change their proposal with each new filing, they still fail to provide a technically feasible approach for delivering the MVPD service to retail devices.

The following sections will review these proposals, note the significant changes introduced with each new proposal, and explain the failure of each to address critical technical issues.

II. PROPOSAL 1: DSTAC WG REPORT – AUGUST 28, 2015

In the DSTAC Report issued on August 28, 2015, which was the culmination of nine months of collective effort, the proponents of the "Competitive Navigation" proposal identified a total of 38 protocols (both existing and/or yet to be either invented or substantially modified) that could be used to implement three "standard" interfaces to the MVPD service.[5] The architecture of that proposal included three primary attributes:

1. The use of only three "standard" interfaces (Service Discovery Interface, Entitlement Information Interface, and Content Delivery Interface) to access the MVPD service.
2. The concept of a "Virtual Headend" that could either implement these three interfaces from the cloud or through a local device in the consumer's home.
3. The lack of a trusted application execution environment in the retail device necessary for security and user interaction.[6]

WG4). For this analysis, we are treating this as a single (although internally inconsistent) proposal. Google and Hauppauge are named as the authors of the device proposal in WG4. *See* DSTAC WG4 Report at 107. Public Knowledge was the primary author of the device proposal in WG3.

[3] Public Knowledge Ex Parte Filing, MB Docket 15-64, October 20, 2015 ("Public Knowledge Oct. 20, 2015 Ex Parte"). In a December 14, 2015 filing in Docket 15-64, INCOMPAS reported that Google had conducted a "technical demonstration." On December 18, 2015, NCTA requested details of which MVPD services were demonstrated, as well as technical standards and specifications, equipment and standards used, a block diagram of all hardware elements and how they were connected from the MVPD network to the display, a list of each protocol stack over each link (e.g. MPEG2 video / XYZ Encryption / MPEG2TS / HTTP / Ethernet); and a list of all software on each device. It asked whether the demonstration showed that the solution would work with all cable, satellite and telco MVPD network architectures and services, or whether it would require changes in network architectures and services. It also asked how privacy, consumer protections, and protection of content and advertising were afforded. Details and answers were never provided.

[4] Consumer Video Choice Coalition (CVCC) Technical Appendix to CVCC Comments, MB Docket 16-42, April 22, 2016 ("CVCC Technical Appendix").

[5] DSTAC WG4 Report at 107-126.

[6] Sidney Skjei, A Technical Analysis of the FCC's Navigation Device Proposal, April 22, 2016, at 6 ("Skjei Technical Analysis") ("In MVPD-supplied devices, the trust infrastructure implements mechanisms to ensure that the trusted application execution environment and the application itself are secured and trusted through various means, such as code signing and tamper resistant software and hardware. Such measures impede the ability of hackers to tamper with the application or trusted application execution environment, which could allow them to compromise the overall security and thereby steal service or steal content.").

An analysis[7] of this original device proposal in the DSTAC Report identified numerous issues with the proposal that made it technically infeasible. Among these numerous issues there were three areas of major technical failings that each subsequent proposal attempted, yet failed, to correct. These three areas are:

- Broken Chain of Trust: Multiple security failings that weaken MVPD security and the associated trust infrastructure.[8]
- New Leased Device Requirement: The requirement for installation of an MVPD-specific device in the home due to the failure for the proposal to technically deliver on its "Cloud-based Virtual Headend" approach.[9]
- Broadcast-only: because the three-stream architecture converts interactive cable services into broadcast-only (one-way) services, the proposal suggested proposed "Widgets" to be invented to address the need to support the user interaction necessary for consumers to complete transactions, such as Video-on-Demand (VoD), Electronic-Sell-Through (EST), and Pay-Per-View (PPV) purchases, user identification, and device registration or association, and future interactive elements of MVPD service.[10]

The subsequent device proposals' approach to these issues changed, yet did not fix or address these failings.

In their October 7, 2015 Comments[11] in support of their DSTAC Report "competitive navigation" proposal the device proponents stated that the technology used in their proposal constituted "mostly" "off the shelf" standards and required "no changes" in MVPD networks to implement and "nothing new" beyond "existing standards and technology 'borrowed' from CableCARD."

Despite these claims of readiness, in their second, October 20, 2015, proposal they dropped 31 of these 38 standards and protocols, retained only 7 of them (though these were mostly minor), and offered 10 new standards.

In their third, April 22, 2016, proposal they offer yet another set of 17 protocols (both existing and/or yet to be either invented or substantially modified), 9 of which (or over half) are newly specified in this latest proposal.

---

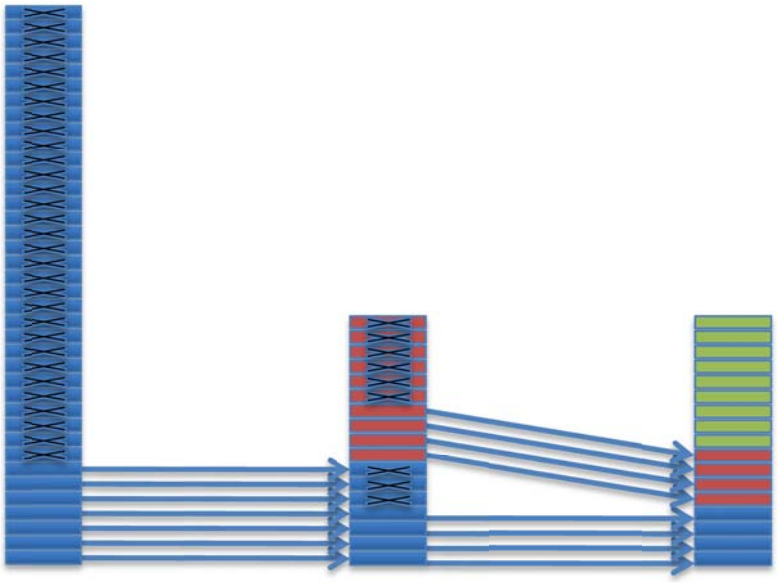
[7] DSTAC WG4 Report at 144-165.

[8] *Id*. at 159 ("The Device Proposal also threatens to undermine the very security that is central to MVPD distribution systems by creating a single national point of attack at the interface.").

[9] *Id*. at 148 ("This forces the MVPD to put a gateway (virtual headend) in the home even if it would be more efficient to use multicast over the access network.").

[10] *Id*. at 144 ("The Device Proposal recognizes that the MVPD UI operates as integral part of service, but then calls for the extraction of discrete elements of the UI, delivered via 'HTML widgets' through an expanded CableCARD MMI that is yet to be invented."); 145 ("The Device Proposal proposes 'to determine the level of HTML that the MMI should support,' but offers no reason why existing specifications like HTML5, EME, MSE and Web Crypto, all developed through the W3C open standards processes, would not be a more appropriate solution, as proposed in the MVPD WG3 and WG4 proposals. Instead, it would require essentially starting from scratch to determine the requirements for the Device Proposal's hypothetical MMI.").

[11] Public Knowledge Comments, MB Docket 15-64, October 7, 2015.



DSTAC Report	Public Knowledge	CVCC
August 4, 2015	October 20, 2015	April 22, 2016

Figure 1 - Changes in Standards Proposed

While the number of standards added and eliminated with each subsequent proposal is noteworthy, it is necessary to analyze the changes in some detail to fully understand the technical implications of these changes.

III. PROPOSAL 2: PUBLIC KNOWLEDGE EX PARTE FILING - OCTOBER 20, 2015

As stated previously, the second proposal dropped 31 of 38 standards, retaining only 7, and adding 10 new ones. Several specific changes in this second proposal are worth highlighting:

1. Elimination of X.509 certificates for security purposes and specifying that the authentication service is optional.[12]
2. Change in the specified discovery protocol from Multicast DNS (through NETCONF and/or Avahi) to UPnP.[13]
3. Elimination of PlayReady DRM and specifying DTCP-IP or DTCP-2 link protection as the only content protection technologies.[14]
4. Elimination entirely of any MMI or "Widget" concept that could support user interaction.

[12] Public Knowledge Oct. 20, 2015 Ex Parte at 3 ("Authentication service is optional.").

[13] *Id*. at 2 ("Overall, the proposed DSTAC implementation is based on various existing UPnP specifications as well as DTCP, which is similar to the DLNA approach generally.").

[14] *Id*. at 2, 3.

An analysis of this second proposal again identified numerous security failings as well as the technical inability to implement a "Cloud-based Virtual Headend."[15]

A. Elimination of X.509 Certificates

The original "Competitive Navigation" proposal contained in the DSTAC Report refers to the use of X.509 security certificates for device authentication.[16] However, as detailed in the analysis of this original proposal, it failed to specify the necessary requirements to actually make these certificates either trusted or useful.[17] In the second proposal, X.509 certificates were eliminated entirely and device authentication was made optional.[18] The ability to disable service to a non-compliant device, as described in the FCC NPRM, requires that device identity and authentication be as reliable and robust as the existing MVPD trust infrastructure. This failure was well documented in NCTA's November 9, 2015 filing.[19] Skjei's technical analysis of the FCC NPRM[20] clearly identifies the requirements for device and user authentication as necessary elements of an MVPD's security systems. Consequently, this elimination of device authentication undermines the security of the MVPD trust infrastructure and also prevents the MVPD from disabling service for non-compliant, including hacked, devices.

B. Change in Discovery Protocol and Elimination of PlayReady DRM

In this second proposal the standard discovery protocol was changed from Multicast DNS[21] to Universal-Plug-and-Play (UPnP).[22] They also eliminated PlayReady DRM from the proposal and

---

[15] NCTA Ex Parte Filing, MB Docket 15-64, January 15, 2016 ("NCTA Jan. 15, 2016 Ex Parte").

[16] DSTAC WG4 Report at 120.

[17] *Id*. at 147 ("The proposal … fails to provide the critical and necessary details about how these certificates are managed, the required trust infrastructure, certification, and any policies necessary to make the certificates useful.").

[18] *See* n.12 above.

[19] NCTA DSTAC Reply Comments, MB Docket No. 15-64, Nov. 9, 2015 at 28 ("NCTA DSTAC Reply Comments") ("[T]he new proposal eliminates DLNA authentication and would require MVPDs to serve unauthenticated devices. Unauthenticated devices are often considered to be pirate devices because they can "share" their credentials widely among other devices – enabling many people to pretend to be the same subscriber using the same device.").

[20] Skjei Technical Analysis at 13 ("*User Authentication*. In order for a device to be associated with a subscriber's account so that the device can enforce the entitlements for that subscriber, the user must be authenticated on that specific device. In order for a subscriber to be securely authenticated, they must provide credentials, typically username and password, via a secure means. In the case of MVPD- provided equipment, (1) the device is associated with the subscriber's account when it is installed in the home, and (2) the device itself includes credentials that identify it and are known by the MVPD (this is the security data referenced in the DSTAC Working Group 2 Report).").

[21] Multicast Domain Name Service (DNS) is the generic term for the method devices on a local network can use to discover the IP address of other devices and services on the local network by name through the use of multicast protocols. The Internet standard protocols Zeroconf and Avahi referred to by the "Competitive Navigation" proposal make use of Multicast DNS. DSTAC WG4 Report at 116.

[22] UPnP is a standard device and service discovery protocol designed for use on home networks as explained in the supporting materials for UPnP. Open Connectivity Foundation, About UPnP, http://openconnectivity.org/upnp (last visited May 22, 2016) ("UPnP technology targets home networks, proximity networks and networks in small businesses and commercial buildings.").

specified DTCP-IP and DTCP-2 link-protection as the single content protection system to be used in both a local gateway-based or cloud-based implementation. Taken together these changes definitively eliminate the possibility of a "Cloud-based Virtual Headend" implementation in this second proposal and require a "Local Virtual Headend" in the form of a secondary MVPD specific device in the home.

More specifically, UPnP is a discovery protocol designed specifically for home networks.[23] Just because UPnP is an IP protocol, it does not imply that UPnP scales to a cloud implementation. UPnP fundamentally works by using only Link-Local and Site-Local scoped multicast messages to which UPnP compliant devices on the link or site-local networks respond with their identification information. This identification information provides a description of the type of device and services supported. This approach does not scale to a network level or even a neighborhood level because each subscriber's home network is a private sub-network. Consequently, these link-local and site-local multicast messages are not forwarded outside the home network. To do so would severely congest the IP network for all users.

Further, DTCP is local link-protection technology that caps the number of devices at less than 35, restricts devices to a set proximity, and it too does not scale to the cloud.[24] DTCP assumes a point to point connection in the home; scaling to a multi-point to multi-point architecture does not scale, even if device number and proximity limitations were relaxed.

The elimination of a "Cloud-based Virtual Headend" implementation means this second proposal still requires that a leased, MVPD-provided server device be placed into the consumer's home and connected to their home network. This "Local Virtual Headend" requirement results in continued device rentals and associated unnecessary energy consumption, especially when compared to zero-STB architectures demonstrated and deployed by cable companies today.[25]

---

[23] The UPnP spec provides that only Link-Local and Site-Local scoped multicast messages may be used. "Devices and control points SHALL NOT send Global scoped, Organization-Local scoped, or Admin-Local scoped multicast messages." UPnP Device Architecture 2.0, section A.2.3 (Document Revision Date: February 20, 2015).

[24] NCTA Jan. 15, 2016 Ex Parte at 2 ("AllVid proponents built their technical proposal on DTCP-IP and UPnP, and that design has significant limitations. CVCC admits that DTCP-IP caps the number of connected devices at 34 and uses localization metrics (measuring round trip time and 3 hops) that do not work with cloud delivery."); 3 ("A change to the DTLA/DTCP license agreement does not solve the problem. To remove these built-in security restrictions would fundamentally change the entire impetus for creating DTCP, and would completely re-write many programming agreements that limit content to in-home consumption.").

[25] Skjei Technical Analysis at 53 ("If one assumes that FCC Devices would enjoy at least the success of the current MVPD app-based approach for iOS and Android devices (56 million downloads), the additional energy utilization across the entire American video viewing footprint would be staggering: 13.42 Terawatts of energy wasted per year, the equivalent to $1.6 billion in increased residential energy bills – over three times more than the gains realized to date under the VA. In terms of environmental impact, this is equivalent to:

- 9 million tons of extra CO2 emissions annually,
- The addition of 4.5 power plants, and
- 2 million more cars on the road.").

C. Elimination of MMI "Widgets" Concept

Another significant change made by the proponents in this second proposal was the elimination of any user interaction capability through the elimination of the "MMI Widget" concept originally described in the DSTAC WG4 Report "Competitive Navigation" proposal.

The original concept made repeated references to a theoretical Man-Machine-Interface (MMI)[26] based on a "widget" model as a cure-all to address any required features and functionalities that could not be implemented through the three "standard" interfaces. The "widget" model was said to be based on the CableCARD MMI which provided only one capability: pairing the CableCARD with the device. However, in their proposal they claimed almost anything "can easily be achieved by the MMI widget model." The "widget" model was invoked whenever a user interaction was required; for example, as necessary to perform VoD purchases or enter a Parental Control PIN, etc. In their original proposal the proponents stated that it was technically feasible for an MVPD to "rebuild" their service from individual "widget" interactions. As described in the DSTAC WG4 Report, it is not technically feasible to do so.[27] The referenced W3C widget specs had already been abandoned by the W3C and all web browsers.

However, beyond the CableCARD MMI reference there was never any detail of how this MMI widget model could actually achieve any of this functionality. One glaring omission, for example, was the support for any standard secure execution environment for the widgets to run in. Absent specificity, the proponents still assured that the widget model could be expected to handle all future innovation. They presumed that each MVPD could disassemble the elements of its service into such widgets, then re-develop, re-test and re-deploy them to rebuild service in this ill-defined environment. The MMI widget model cannot share data among "widgets," there is no way for "widgets" to coordinate on sharing the screen real estate and there no way to share control of the input device (TV remote).

Even if a "widget" specification was invented and implemented, the resulting MVPD user interactions could be blocked by the device manufacturer. In the October 20, 2015 filing by Public Knowledge, the proponents abandoned the "widget" model.

As detailed in Skjei's technical analysis of the FCC set-top NPRM, the absence of a well-known trusted application execution environment in which to implement interactive and User Interface features undermines the service delivery, consumer protections, and security of the MVPD's trust infrastructure.[28]

---

[26] DSTAC WG4 Report at 118.

[27] *Id*. at 144 ("The Device Proposal recognizes that the MVPD UI operates as integral part of service, but then calls for the extraction of discrete elements of the UI, delivered via "HTML widgets" through an expanded CableCARD MMI that is yet to be invented. The CableCARD MMI does not define how a hyperlink is navigated and selected. Unlike the application environment we see today, the CableCARD has no provision for JavaScript or other application execution environment in the Host device on the other side of the CableCARD interface. The Device Proposal suggests the potential for interactivity in an expanded MMI, but as the proposal stands today it does not offer any specifics; does not promise any capability for maintaining state information in the retail device necessary for application data to persist across widgets instances of the capabilities of this MMI; and provides no retail device query capabilities for adapting to different retail devices to different MVPDs. An MMI has to have an execution environment in the client to provide any form of interactivity, or it fails. But the Device Proposal provides for no execution environment within which the widgets delivered through the MMI can operate.").

[28] Skjei Technical Analysis at 5-9.

D. Other Technical Issues in the Public Knowledge Ex Parte Filing

In this second proposal, the proponents assured that the October proposal used "standards and specifications in common use by MVPDs today."[29] However, this is not the case, as was thoroughly documented in NCTA's November 9, 2015 reply comments.[30] The October proposal called for UPnP approaches that are not "in common use by MVPDs today," and have not been proven through common adoption across all MVPDs. It relied on DLNA EPG Guidelines that were abandoned by DLNA, were never implemented, and consequently are also unproven.[31]

The proposal cannot "be described and referenced in accordance with the tools comprising DLNA CVP-2" nor would it "draw on independent certification tools and bodies already in existence" as had been claimed in the proposal.[32] It did not "most resemble VidiPath" or use "independent certification tools and bodies already in existence … at minimal burden," as had also been claimed. This proposal eliminated the Remote User Interface (RUI) requirements of the VidiPath Guidelines, making the server, not the app, the adaptation point, and called for a new, unspecified architecture different from VidiPath. With these fundamental changes to the VidiPath Guidelines, the DLNA certification tools would need to be redeveloped, are unproven, and are not testable by existing DLNA certification processes. The proposal would also require major development, testing, and certification efforts on the part of MVPDs to create a new hardware device in the home.

IV. PROPOSAL 3: TECHNICAL APPENDIX TO CVCC COMMENTS - APRIL 22, 2016

Now, through the CVCC Technical Attachment, the device proponents offer yet another set of 17 protocols (existing or to be invented), 9 of which (or over half) are newly specified in this proposal. The specific changes in this latest proposal worth highlighting:

1. Adds Microsoft PlayReady and Google Widevine as mandatory DRMs, as well as DTCP-HE to the proposed content protection systems.[33]
2. Adds requirements for Common Encryption and mandates support for key exchange with the mandated Google Widevine or Microsoft PlayReady DRM clients.[34]

---

[29] Public Knowledge Oct. 20, 2015 Ex Parte at 1.

[30] NCTA DSTAC Reply Comments at 27, 28-29, 35-36.

[31] Digital Life Network Alliance (DLNA) Comments, MB Docket No. 16-42, April 22, 2016 ("In reference to the specific DLNA Guidelines mentioned in the filing by John Bergmayer, MB Docket No. 15-64, October 20, 2015, it should be noted that 'upnp:EPG feature and cds:EPG class described in DLNA Guide- lines Part 1 Section 5.7.15 and Part 1 Section 1.7.4.4.11' have no certification program. Testing and certification programs are essential for consumer confidence and device interoperability.").

[32] Public Knowledge Oct. 20, 2015 Ex Parte at 1.

[33] CVCC Technical Appendix at 2 ("Through an appropriate content protection method (such as DTCP-IP, DTCP-HE, DTCP-2, Widevine DRM, or PlayReady DRM), the content is protected between the server and clients.").

[34] *Id*. at 4 ("Common Encryption should be used for DRM, with support for either Widevine or Microsoft PlayReady DRM clients for key exchange. Alternate DRMs may also be used, as long as they utilize Common Encryption and also provide support for key exchange with either Widevine or Microsoft PlayReady DRM clients.").

3. Adds back requirements for device certificates, but with no reference to the DSTAC WG4 Report's previous discussion of certificates, as well as specific requirements for certificate handling through HTTP headers.[35]
4. Proposes a new architecture and approach for a "Cloud-based Virtual Headend" using WebSockets and OAuth2 tokens.[36]

The net of all of these changes are that none of the key issues identified in the earlier proposals have been addressed and the latest proposed security elements are weaker than their prior proposals. The following issues originally identified in the DSTAC Report remain:

1. Numerous security failings.
2. Lack of a trusted application execution environment and inadequate support for user interaction.
3. The requirement for an MVPD specific device in the home.

A. Numerous Security Failings

One of the numerous security failings is mandating support for two specific DRMs regardless of their robustness. Further, they propose to mandate that any other DRM an MVPD may choose must exchange keys with either Google Widevine or Microsoft PlayReady, making these two DRMs by definition the weakest link. While key sharing is an important tool, it needs to remain within the control of the MVPD responsible for the secure distribution of the programming. This third proposal further weakens security by mandating key sharing with these two chosen DRM systems, whether or not an MVPD has selected them for security. In addition, Google Widevine is affiliated with the MVPD Google Fiber TV and would be disqualified as an "unaffiliated" content protection system under the NPRM. That leaves one specific point of failure – a weak link independent from the Compliant Security System(s) selected by the MVPD that are nonetheless capable of jeopardizing the security of every other MVPD's services via a single breach. If either DRM is hacked, all systems are exposed. This lowers the overall robustness of the security regime.

This proposal ignores both the danger of creating single points of failure and the basic design of the modern apps-based security system that promotes strategic diversity and competition in security solutions. One of the most basic tenets of security design is that single points of failure undermine overall security for all participants. This was one of the major points of agreement during the DSTAC process, which reached consensus on the principle that any recommendations should "avoid rigid and/or single implementations (one-size-fits-all) that significantly limits innovation, competition, or increases security risk."[37] In addition, should one of these two mandated DRMs be hacked, fail to keep up with ever-increasing levels of security, or simply exit the business, there is no discussion of how the ecosystem recovers.

---

[35] *Id*. at 5 ("All HTTP requests made to the server over any of the three information flows must include an HTTP header that specifies the URL that hosts a webpage that indicates compliance with all the aspects of the Certificate as specified in the NPRM.").

[36] *Id*. ("In order to enable delivery of UPnP events from cloud-based servers, an extension to the UPnP event mechanism will be added utilizing WebSockets.").

[37] DSTAC WG3 Report at 18.

With respect to the DRM server that is responsible for the key delivery, the CVCC proposal would require the IP address of any DRM license server(s) to be advertised via the CDS on the home network.[38] This exposes the DRM license server to greater potential attack as the DRM license server itself is advertised in a standard format to any third party that has access to the subscriber's home network, thereby exposing those servers even further to hackers and undermining overall security. There is nothing to prevent malware on a subscriber's computer to easily discover and exploit this vulnerability.

Another security shortcoming is the selection of an unproven technology that has not undergone peer review by security experts. The "DTCP-HE" reference[39] is to a proposal made by Alcatel-Lucent in June 2012 that has not been adopted by DTCP, was never proposed to or reviewed by the DSTAC working group specifically designated to review security proposals (WG3), does not appear to have received a security vetting by third-party security experts, and represents a completely new DTCP security protocol.

Another large security failing is the proposed certificate handling requirements.[40] It proposes that the header of each HTTP request contain a URL that hosts a webpage that indicates compliance. There is no method by which this URL can be validated. A pirate or hacked device or rogue app would simply substitute the URL for a known compliant device or app in its HTTP requests to masquerade as the compliant device or app. In human parlance, this is called "identity theft." Even if there were a means of validating that the URL contained in the HTTP requests actually represented that device or app, one can only assume that through CVCC's insistence on self-certification, the certificate retrieved from the specified URL would be a self-signed certificate. Self-signed certificates are well-known security vulnerabilities, as when used in SSL connections, for example.[41] A self-signed certificate only asserts that the entity that signed the certificate claims to be who they say they are and asks that you trust that assertion. There is no third party to validate that this assertion is in fact true. Any entity, including hackers, can generate self-signed certificates.

Lastly, there is nothing in this proposal to prevent users from sharing credentials (e.g. user name and password) with others who do not have a subscription from the MVPD. The use of OAuth2 tokens for security purposes in a cloud-based implementation is not a guarantee of security, as

---

[38] CVCC Technical Appendix at 4 ("When DRM is used for content protection, the DRM license server should be specified in the DASH manifest or be specified in the CDS using the *DRMInfo:foreignMetadata* property. When an in-home MVPD device is used for providing the Service Discovery Interface, then it also must act as a proxy to the DRM license server for the DRM key exchange and perform all authentication with that license server itself.").

[39] *Id*. at 2.

[40] *Id*. at 5 ("All HTTP requests made to the server over any of the three information flows must include an HTTP header that specifies the URL that hosts a webpage that indicates compliance with all the aspects of the Certificate as specified in the NPRM. Requests that do not contain this URL, contain an invalid URL, or contain a URL that has been deemed to be from a non-compliant source should be rejected.").

[41] Thawte, Inc., The Hidden Costs of Self-Signed SSL Certificates, 2013, https://www.thawte.com/assets/documents/whitepaper/hidden-costs-self-signed-ssl-certificates.pdf at 3 ("Self-signed certificates are inherently less trustworthy than those signed by leading CAs. Reputable third-party CAs have robust processes in place to help ensure that their encryption keys, especially their highly sensitive private "root" keys, are kept safe. For these CAs, security is always a top priority: Personnel are rigorously vetted and highly trained, and these CAs have strict policies concerning where private keys are stored. In fact, if a CA wants to be approved by mainstream web browsers, these keys must be kept on non-extractible storage on smart cards.").

recent press[42] demonstrates how a retail device manufacturer's improper use of OAuth tokens allowed attackers to take control of a consumer's smart lock and unlock their front door.

The CVCC proposal also introduces a new concept of a third-party MVPD registry, which is suggested to be similar to how consumers log into authenticated programmer websites like HBO.[43] However, this proposal conflates authentication via a trusted third party, the programmer website and authentication via an unknown third-party device. A login through a programmer website is trusted because they are partners in contract and equally invested in security and preventing theft of service. The third-party devices that the FCC NPRM and the CVCC proposal describe are by definition not part of the MVPD trust infrastructure, and under no contractual obligation with the content provider to protect the content. Consequently, a login via the proposed registry is less secure.

Security calls for a stronger certification program than simply self-certification. In order to reliably attest to the compliance of a device or implementation in accordance with a standard or specification, some form of third-party testing must be performed; otherwise, devices manufactured to specifically circumvent the standards or specifications can simply falsely assert their self-certification. Testing and certification procedures are widely used to provide distributors, developers, consumers, and retailers the assurance that the platform, devices, and applications designed for them will actually work. A good example is HDMI. Differing CE implementations of HDMI led to a cacophony of non-interoperable "standard" interfaces that finally was sorted out in December 2006, when Best Buy demanded a new "Simplay HD" testing and certification regime for CE devices. Other examples include: DLNA certification of TVs, mobile devices, and other consumer devices; retail DOCSIS modems are subjected to a full certification process; the Wi-Fi Alliance tests and certifies 802.11 equipment; and others use comparable regimes.

B. Inadequate Support for User Interaction

Originally, in the DSTAC report, proponents sought to address the failure of their proposal to support critical interactive elements of service with an undefined "widgets" concept. In the October 20, 2015 ex parte there was no mention of HTML5 or Widgets, and now, in their most recent technical attachment, they introduce the concept of a "web browser" reduced to a single functionality – to address VoD transactions and user authentication.[44] This back-and-forth on MMI, Widgets, or stripped-down Web Browsers makes clear the fundamental issue the proponents are trying to dodge: retail devices must provide some trusted application execution environment on the client. This fundamental concept of content streaming security is also

---

[42] Dan Goodin, *Samsung Smart Home flaws let hackers make keys to front door*, Ars Technica, May 2, 2016, http://arstechnica.com/security/2016/05/samsung-smart-home-flaws-lets-hackers-make-keys-to-front-door/.

[43] CVCC Technical Appendix at 5 ("Any implementer who creates a cloud-based server must post on its website the URL utilized to access the Service Discovery Interface (the expectation here is that these URLs will be aggregated by a third party to enable programmatic lookup of them)."); *id*. ("Authentication to the cloud-based server located at 5(a) should be done via techniques similar to what MVPDs use for TV Everywhere login (i.e., either automatic or via webpage login with their MVPD credentials).").

[44] *Id*. at 3 ("This information will either consist of a URL for performing the purchase process via a web browser or use a vendor-specific UPnP action that may require entry of a customer specific PIN code for directly purchasing the content."); 5 ("Authentication to the cloud-based server located at 5(a) should be done via techniques similar to what MVPDs use for TV Everywhere login (i.e., either automatic or via webpage login with their MVPD credentials).").

detailed in Skjei's technical analysis of the FCC NPRM.[45] Yet the latest inclusion in their proposal of a stripped-down "web browser" in order to narrowly address the VoD transactional functions and authentication requirements does not satisfy the requirement for a trusted application execution environment. This proposal suffers from the same technical issues as the original "Widget" model described in the DSTAC WG4 Report and discussed above. This proposal lacks any detailed specifications of the web browser's functionality as well. It does not address the various forms of VoD transactions, e.g. free VoD, subscription VoD, transactional VoD, LookBack, StartOver and Electronic Sell Through. A simple PIN entry is not sufficient to address all of these forms of VoD. The absence of a predictable execution environment eliminates the possibility of providing an enforceable or auditable way to handle VoD purchases, which must be validated through to the user interaction on the receiving device. The resulting security risks are also described in Skjei's technical analysis of the FCC NPRM.[46]

C. Requirement for an MVPD Specific Device in the Home

The specification of Universal Plug and Play (UPnP) "Content Directory Service" (CDS) and DLNA Digital Media Server (DMS)[47] requires that the CDS and DMS be implemented in an MVPD-provided device located physically on the home network. The cloud-based solution they propose[48] requires an entirely new set of protocols based on OAuth2 and WebSockets. WebSockets creates a two-way communication channel between the client device in the home and a server in the cloud. It does not define the format or content of the data that is exchanged between the two using this WebSocket. The applications on either side of the WebSocket must agree on this and be coded appropriately in order for the two to interoperate properly. Simply identifying WebSockets as a communication mechanism is insufficient. Further, using this WebSocket approach, the retail device is unable to participate in any UPnP interactions that span both the home network and the WebSocket to the cloud. For example, this approach breaks the UPnP "three box model" in which the AV Control Point (the device that acts as the remote control) is a different device from either the Media Server (the device that is the content source, in this case, the cloud) or the Media Renderer (the device that displays the content or the retail device). The AV Control Point would be required to have its own separate WebSocket to the cloud. In this scenario, there is no method to coordinate the two communications channels as the cloud Media Server would have no way of identifying the two WebSockets as being part of a three-way conversation.

Beyond the use of an OAuth2 token, the proponents do not discuss if or how traffic on this WebSocket is protected. This is a major privacy and security hole since it carries all of the user traffic (requests to both the CDS and DMS) between the user and the cloud-based servers. Left unprotected, hackers can observe, collect, monetize, or exploit subscriber viewing habits.

---

[45] *See* n.28 above.

[46] Skjei Technical Analysis at 11 ("The lack of a trusted application execution environment could permit hackers to compromise these VOD transactions and requirements.").

[47] CVCC Technical Appendix at 3.

[48] *Id*. at 5 ("In order to enable delivery of UPnP events from cloud-based servers, an extension to the UPnP event mechanism will be added utilizing WebSockets. This will establish a bidirectional HTTP link to enable clients sending requests to the server and the server also sending events as HTTP requests back to the client (i.e. both endpoints of the WebSocket connection will be an HTTP Server and an HTTP Client where SUBSCRIBE, UNSUBSCRIBE, and NOTIFY messages will be sent).").

Further, this proposal doesn't address network latency and bandwidth contention on the MVPD broadband access network. UPnP is a notoriously "chatty" protocol (a lot of back-and-forth communications between client and server) and while it works across a home network, it is unclear how it scales over a wide area network. In addition, this would require an MVPD to implement UPnP/DLNA functionality in their networks and it is unclear how many servers they must host (potentially one per subscriber or retail device) for purposes of terminating the server side of this WebSocket connection.

Finally, there is no assurance that the UPnP and DLNA guidelines as specified by the CVCC Technical Attachment are actually implementable, since there has never been a test, certification and validation program created for such a combination of them. It is common practice in the standards setting process to build, test, and verify newly created standards.

D. Other Technical Issues in the Technical Appendix to CVCC Comments

The CVCC comments themselves identify a proposed additional parity requirement that applies to the number of simultaneous available streams.[49] Specifically, CVCC proposes that retail devices must be able to support the same number of simultaneous streams as MVPD provided devices. This proposal assumes that the number of simultaneous streams is a fixed number, and parity demands that at least this fixed number of streams be available to retail devices. However, in some MVPDs' systems the number of simultaneous streams is not fixed and is actually dynamically determined through proprietary protocols combined with the type (SD, HD, or UHD) and number of actual video streams being consumed. Consequently, the parity requirement cannot be met unless the retail device implements these proprietary protocols as well. Yet the NPRM mandates that only open standard protocols are used, thus preventing this additional parity requirement from being met.

CONCLUSION

Each proposal, including the approach proposed in the NPRM, shares three fundamental common failings:

1. Broken Chain of Trust: they all include multiple security failings that weaken MVPD security and the associated trust infrastructure.
2. New Leased Device Requirement: they all require installation of an MVPD-specific device in every MVPD home due to the failure for the proposal to technically deliver a "cloud-based" approach.
3. Broadcast-only: they all rely on a three-stream architecture that reduces interactive cable services into broadcast-only (one-way) services, removing the necessary support for essential aspects of MVPD service such as Video-on-Demand (VoD), user identification, and device registration, and other interactive elements.

[49] CVCC Comments, MB Docket 16-42, April 22, 2016 at 32 ("Discovery data should include information on the number of simultaneous available streams. Parity regarding the number of tuners should be required for devices that support Service Discovery and those that do not.").

The proponents' inability to address the fundamental problems created by "unbundling," notwithstanding the intense work undertaken since the beginning of the DSTAC process in January 2015, indicates that the "Competitive Navigation" proposal is technically infeasible.

The root problem is that all of these proposals have abandoned the applications and trust infrastructure that is a foundational requirement for modern MVPD service. By contrast, apps-based solutions that operate within the trust infrastructure are already operating in the market and do provide retail device support, as detailed in the DSTAC Report.[50]

[50] DSTAC WG4 Report at 127-135.

APPENDIX B

SELECTION OF PROGRAMMER APPS

APPENDIX B – SELECTION OF PROGRAMMER APPS

Figure 1: Individual Apps Available from Programmers in Addition to MVPD Apps offering the MVPD Service

Figure 2: Sample Programmer Apps on Display at INTX 2016

Figure 3: More Programmer Apps on Display at INTX 2016