Before the
Federal Communications Commission
Washington, DC 20554

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

Comments of the Electronic Frontier Foundation

April 22, 2016

The Electronic Frontier Foundation (EFF) appreciates the Commission's efforts to achieve the goal that Congress set out twenty years ago: to "assure" that consumers can access television programming from their multichannel video provider (MVPD) on the devices of their choice.[1] We especially welcome the Commission's commitment to establishing a competitive marketplace for navigation devices based on open standards.

EFF is a member-supported, nonprofit, public interest organization promoting individual rights and empowering innovation in the digital world. Founded in 1990, EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers. EFF has contributed its expertise in law, regulation, and technology to issues of innovation and competition in video technology for many years, including participation in working groups on video copy controls and representing consumers on the issue of competition in MVPD end-user devices.[2] Our work focuses especially on the interaction between FCC regulations and intellectual property law.[3]

MVPDs remain the primary source of home video entertainment for millions of Americans. Many popular programs are available *only* through an MVPD. At the same time, the MVPD industry is growing ever more concentrated in the hands of a small number of companies, many of whom bundle pay-TV service with broadband Internet access. And home equipment for receiving pay-TV is ever more integrated with other personal technology, multiplying the importance of privacy and security.[4]

[1] Telecommunications Act of 1996, Pub. L. No. 104-104, § 304, 110 Stat. 56, 125-26 (1996); 47 U.S.C. § 549.

[2] *See* Derek Slater, *Another Step Towards Cable Set-Top Competition*, EFF Deeplinks Blog (Jan. 11, 2007), https://www.eff.org/deeplinks/2007/01/another-step-towards-cable-set-top-competition.

[3] *See* "Broadcast Flag," https://www.eff.org/broadcastflag; "WNET v. Aereo," https://www.eff.org/cases/wnet-v-aereo.

[4] For example, Mediacom integrates VOIP phone service and Caller ID with its set-top boxes. Home Phone Features, https://mediacomcable.com/site/phone_features.html (accessed April 21, 2016). Time Warner.

All of these developments make opening MVPD end-user hardware and software to true competition more important than ever. Competition means more than just lowering prices for consumers. It drives innovation in features at every level: in hardware, software, user experience, energy efficiency, security, and cost. It allows consumers to vote with their dollars along many dimensions of preference: ease of use, sophistication of search, recommendation, and program discovery features, integration of multiple sources of programming, respect for privacy, and security, including the ability of third parties to perform security audits.

The Unlock the Box rules could unlock competition along all of these dimensions. By contrast, rules that merely spur some measure of increased price competition but allow MVPDs and their partners to preserve monopolistic control over the *design and functionality* of such devices will fall short. If the Commission's 1968 *Carterfone* decision[5] had permitted new competitors to sell telephones but limited them to selling phones that were substantially similar to the phones leased by AT&T, that decision would not have spurred so many advances in phone technology, from the fax machine to consumer-level data modems that brought the Internet to a broader public. Competitive video navigation devices and software cannot be a true market alternative to MVPD-leased boxes if their features, interfaces, and design are constrained by the MVPDs' preferences, even if those preferences are cloaked in the language of security, robustness, or content protection.

We submit these comments to address statements made by MVPDs and major television producers (who have generally opposed every attempt to implement the mandate of Section 629) concerning the role of copyright law. We also suggest approaches to consumer protection, particularly privacy. While these are issues of vital importance, none of them present a serious obstacle to this rulemaking.

In addition, we discuss a component of navigation device competition that this rulemaking should address: discouraging the misuse of anti-circumvention law (particularly Section 1201 of the Digital Millennium Copyright Act)[6] to suppress independent security research that can protect consumers.

1. MVPDs Have No Statutory or Regulatory Right to Control the End-User Interfaces Used to Access Lawfully Obtained Video Content, and the Commission Need Not Create One.

As it moves forward with this rulemaking, the Commission should not be deterred by exaggerations of MVPDs' legal rights (or legitimate expectations) to control the user experience. The Commission should resist the efforts of MVPDs to blur two separate issues: (1) prevention *unauthorized access* to pay-TV content; (2) and control over design

---

Cable integrates "Indoor-outdoor cameras, motion detectors, smart door locks, flood detectors and more." IntelligentHome from Time Warner Cable, http://www.timewarnercable.com/en/intelligenthome/overview.html (accessed April 21, 2016).

[5] *In the Matter of Use of the Carterfone Device in Message Toll Tel. Serv.*, 13 F.C.C.2d 420, 421 (1968).

[6] 17 U.S.C. § 1201.

and functionality of end-user hardware and software. The Commission should treat these separately, because only the former is protected by law, while the latter is at the heart of the competition that Congress intended Section 629 to enable.

a. The Unlock the Box Rules Do Not Affect the Status or Enforcement of Copyrights, nor Permit Unauthorized Access to Programming.

Nothing in the proposed rules permits any party to obtain unauthorized access to programming. Specifically, nothing in the proposal requires MVPDs to make programming available to any devices or apps where the customer has not subscribed or purchased access to that programming. Providing "Entitlement Data"[7] to the navigation device does not imply that the MVPD must transmit any programming to the device for which the customer has not paid.

Nor do the proposed rules authorize any party to copy or distribute TV programming in violation of copyright law. Just as an MVPD must comply with the Copyright Act or obtain a copyright license from rightsholders in order to make public performances of TV programming, so must any potential vendor of competitive navigation devices or apps.

Compliance with FCC regulations (or lack thereof) does not determine whether a service or technology vendor is in violation of copyright law, except in a few circumstances where the Copyright Act says so explicitly, such as eligibility for the Section 111 and 119 statutory licenses for broadcast programming.[8] Outside of those well-defined circumstances, nothing the Commission does can or will alter the copyright status of any MVPD, technology vendor, add-on service, or customer.

The functions of an end-user navigation device or app don't fall within the exclusive rights of a copyright holder. Selling devices to consumers to *receive* television broadcasts does not implicate any of the exclusive rights set forth in the Copyright Act, as such devices do not publicly perform TV shows,[9] nor do they reproduce them (aside from transitory copies commonly made when computers handle video files). Nor do providing recording devices[10] or remotely operated personal recording *services*[11] fall within a rightsholder's power to prohibit or condition. Again, these acts are lawful regardless of whether the Commission acts or not. The Unlock the Box rules would, however, allow new competitors to sell the hardware, software, and services that enable these lawful functions.

[7] Notice of Proposed Rulemaking and Memorandum Opinion and Order ¶ 39 ("NPRM").

[8] *See* 17 U.S.C. § 111(c)(2)(A); § 119(a)(1)-(2).

[9] *See Fortnightly Corp v. United Artists Television, Inc.*, 392 U.S. 390, 398 ("Broadcasters perform. Viewers do not perform.").

[10] *Sony Corp. of Am. v. Universal City Studios, Inc.,* 464 U.S. 417, 456 (1984).

[11] *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 140 (2d Cir. 2008).

Copyright law is no obstacle to the proposed rules.

b. MVPDs Have No Legal Right or Reasonable Expectation to Control User Interfaces.

As the proposed rules do not affect the statutory rights of MVPDs or rightsholders under copyright law, these entities have sought to blur the distinction between their statutory rights (e.g., the right to limit unauthorized copying or public performance) and their ability to leverage those rights into control over unrelated areas of hardware and software design, such as program search and discovery functions. This distinction is vital, because allowing non-MVPD-affiliated technology vendors to compete in the market for end-user navigation devices and software *without* an effective veto by MVPDs is the essence of Congress's command that is the impetus for this rulemaking.

Representatives of major television and movie studios have claimed in letters to the Commission and in public statements that allowing companies independent of MVPDs to create new user interfaces for MVPD subscribers amounts to "companies profiting from content they haven't paid for,"[12] or "creat[ing] a new service without license or compensation to content owners."[13]

This position is nonsensical as a matter of law, history, and logic. Copyright law grants no right to control "profiting from content" or "creating a new service" when the rights of reproduction, distribution, etc. are not implicated,[14] or when fair use applies.[15] Numerous industries, from TV and DVR manufacturers to home and vehicle audio installers to popcorn growers "profit" from the demand for creative work without permission or payment to copyright holders.

This is not a flaw in the legal system but a vital feature, as it allows for independent innovation from diverse sources. For decades, decisions of the Supreme Court have emphasized the need to avoid expanding the copyright monopoly into "substantially unrelated areas of commerce" and to avoid placing unnecessary constraints on innovation.[16] Congress and the courts have already determined that giving copyright holders control over end-user equipment is not necessary to create incentives for creative

[12] Neil Fried, "The FCC Should Say 'No' to AllVid: Part Two," Motion Picture Association of America Policy Focus (Feb. 3, 2016), http://www.mpaa.org/allvid/.

[13] Letter from Rick Chessen, Senior Vice President, National Cable and Telecommunications Association to Marlene H. Dortch, Secretary, Federal Communications Commission, at 1-2 (Jan. 15, 2016) ("NCTA Ex Parte").

[14] *Cartoon Network*, 536 F.3d at 140.

[15] *Fox Broad. Co. v. Dish Network LLC*, No. CV 12-4529 DMG SHX, 2015 WL 1137593, at *21 (C.D. Cal. Jan. 20, 2015) (holding that personal DVR use is a fair use).

[16] *Sony*, 464 U.S. at 442; *see also Am. Broad. Companies, Inc. v. Aereo, Inc.*, 134 S. Ct. 2498, 2510, 189 L. Ed. 2d 476 (2014) ("Congress . . . did not intend to discourage or to control the emergence or use of different kinds of technologies").

work. The courts have also made clear that copyright is not a license to engage in anticompetitive practices.[17]

In light of this history and precedent, business and contractual arrangements among major MVPDs, TV studios, and others should not stand as an obstacle to enacting the Unlock the Box rules simply because those arrangements involve copyright licenses.

Under the proposed rules, MVPDs and rightsholders will continue to be able to enter contracts for their mutual benefit with respect to channel placement, user interface design, and advertising within the user interface of the navigation devices sold or leased by MVPDs. The proposed rules will permit independent makers of navigation devices and software to compete with MVPDs for those contracts. With a true choice of user interfaces, including search and discovery functions, customers will be able to decide which forms of channel placement and other design choices serve them best. Any unhelpful or unappealing design choices will likely fail in the market. Any deceptive or misleading features or practices, including those with respect to advertising, will be subject to broadly applicable consumer protection laws.

2. Navigation Device Rules Can and Should Protect Consumers.

EFF agrees that the navigation device rules must not undermine consumer protection goals.[18] While the Commission should proceed cautiously, effective consumer protection, as with copyright, need not be an obstacle to achieving the goals of this rulemaking.

First, EFF believes that self-certification of consumer protection requirements for competitive navigation devices and software is reasonable if the self-certification is published and made widely available to consumers. For example, expanding on the suggestion in ¶ 74 of the NPRM, the Commission, the Federal Trade Commission (FTC), or both agencies together, could maintain websites that publish or link to the most current self-certifications so that all consumers, businesses and government entities can easily satisfy themselves that vendors are protecting their privacy.

Competitive device vendors are not common carriers exempt from FTC jurisdiction, and the proposed certification of adherence to the privacy protections of 47 U.S.C. §§ 551, 338(i) would be a material representation subject to the FTC's authority over unfair, deceptive or misleading trade practices.

We strongly doubt that a competitive market can protect consumer privacy without strong transparency mechanisms like public certification, because so much of privacy protection depends on behavior that consumers cannot "see" or verify, such as collecting data from device streams, data retention, and data sharing.

[17] *United States v. Microsoft Corp.*, 253 F.3d 34, 63 (D.C. Cir. 2001).

[18] Because EFF does not work in the general policy area of children's protection, we do not comment on children's programming advertising restrictions.

By contrast, it will be fairly easy to determine whether, for example, closed captioning is provided, and we expect vendors to proudly trumpet EAS messaging capability and thus put pressure on the rest of the market.

If MVPDs are given the authority to certify compliance with consumer protection rules, or the ability to influence independent certification, certification would become yet another avenue of MVPD control over nominally independent devices.

As to whether independent certification of privacy and other consumer protection concerns is appropriate, we express no opinion at this time except that we believe it should be optional at most. Our primary concern is that such third-party certification be truly independent, so that MVPDs can never influence certifications.

EFF believes the Commission may require that MVPDs provide the Information Flows only to self-certified competitive device vendors. Without privacy assurances and transparency, consumers might avoid competitive devices, which could significantly hinder competition given the typical costs of shifting from the "easy" default of using MVPD-provided equipment. The main issue is to ensure that the certification regime is exactly that—a simple way for competitive device vendors to make public, accountable claims that they adhere to the relevant privacy rules—and not an additional avenue for regulatory gamesmanship by MVPDs.

We are thus concerned about the discussion of device authentication in ¶ 76. At this time, we are not aware of any particular need to regulate on this issue. Indeed, our main consumer protection concern here is that MVPDs may unnecessarily raise the price and transaction costs of using competitive devices by seeking unnecessary device authentication requirements.

But if the Commission can establish a genuine need for device authentication, then it should be done with a light hand, such as with a vendor-set "flag" or "code" during the set-up process signifying that the device has been certified by the manufacturer to conform to the requirements.

While we support the idea that MVPDs would not be required to enable the Information Flows to a device revealed to be non-compliant with the privacy certification, the Commission should emphasize that MVPDs are not required to disable Information Flows in such a case.

More generally, we do not support the premise behind the Commission's question, "how can MVPDs ensure, as both a technical and practical matter, that the Information Flows are no longer provided if there are any lapses in a competitor's compliance with these obligations?"[19] Our greatest disagreement is with the phrase "any lapses in a competitor's compliance." There is no reason to believe that the consumer's incentives or interests here coincide with those of the MVPDs.

[19] NPRM ¶ 76.

The consumer or end-user has a strong interest both in privacy and in getting the benefits of the device they have purchased. A consumer who is counting on a DVR recording should never lose access through their chosen device merely because the MVPD decides that the competitive device is uncertified or has gone out of compliance. At a minimum, lapses justifying a cut-off of the Information Flows must be severe, consumers must be notified at least several days in advance of the cut-off, and consumers must be able to waive non-compliance and avoid a cut-off.

On the question of state law, California's Business & Professions Code § 17200 exemplifies a state-based consumer protection regulatory scheme. Section 17200 creates a private right of action against unlawful, unfair, or deceptive trade practices for consumers with evidence of economic harm, and also can be enforced by a variety of state and local officials with no showing of harm.

There is much literature and case law on § 17200, but its most important features include:

- a remedy for behavior that is statutorily "unlawful," even if the relevant statute has no private right of action.
- claims that can reach discontinued conduct.

In addition to the state attorney general, any district attorney, any city prosecutor, and city attorneys of large cities (over 750,000 population) can bring § 17200 actions. Civil remedies under the private right of action are limited to injunction and restitution, and § 17200 does not itself provide for attorneys' fees, although they can be recovered under independent theories.

3. Open Standards Bodies Should Protect and Promote Independent Security Testing Of Navigation Devices.

a. Navigation Devices Are High-Value Targets for Attackers.

Today's set-top boxes and other video navigation devices are powerful computers. They often have prodigious local storage (for video recording functions), graphics co-processors, multiple network interfaces, large amounts of random-access memory, and, increasingly, sensors, including cameras and microphones to enable voice and gestural control, as well as gaming.

Set-top boxes are networked. They are often merged with Residential Network Gateway devices supplied by the MVPD as part of a bundled MVPD and broadband service. These devices sit at the interface of the public Internet and customers' home networks, which connect security systems, CCTVs, baby monitors, networked thermostats, and the whole realm of Internet of Things devices, not to mention the laptops, phones and tablets that households use to send and receive sensitive, private data.

Set top boxes are widespread. More than 80% of American households have some form of pay TV.[20]

The combination of these three facts makes set-top boxes and other video navigation devices—both MVPD-provided and competitive—into high-value targets for malicious attackers.

b. Information Security Is Difficult, and Must Fail Gracefully.

Pre-release testing, no matter how robust and exacting, cannot ever fully secure a system. As cryptographer Bruce Schneier says, "security is a process, not a product" because "anyone can design a security system that works so well that he himself can't figure out a way around it."[21] It's only when security systems are tested by other creative intellects, with different strengths and points of view, that the oversights in the designer's assumptions can be surfaced.

It is comparatively easy to make systems that work well, provided one doesn't care how they fail. We anticipate that navigation device manufacturers will do their level best to secure their systems prior to shipping, but a device that passes initial testing might still permanently cease to function because of undiscovered defects,[22] or be vulnerable to remote attacks.[23]

c. Disclosure Is Key to Failing Gracefully.

Disclosure of security vulnerabilities has long been the center of controversy, but there is a consensus among security experts that independent testing by diverse researchers is vital to the remediation of defects and continuous improvement of security.[24]

[20] Leichtman Research Group (LRG), "Pay-TV Penetration Rates, 2010-2015," MarketingCharts.com (Sep. 9, 2015) http://www.marketingcharts.com/television/pay-tv-penetration-rates-2010-2015-58837/.

[21] Bruce Schneier, "Schneier's Law," Schneier on Security (April 15, 2011), https://www.schneier.com/blog/archives/2011/04/schneiers_law.html.

[22] Mark Frauenfelder, "Why 1/1/1970 Bricks Your iPhone," Boing Boing (Feb. 16, 2016), http://boingboing.net/2016/02/16/why-111970-bricks-your-iphon.html.

[23] Xeni Jardin, "Dick Cheney Feared Assassination by Cardio Device Hack, Had Docs Turn Defibrillator's Wireless Off," Boing Boing (Dec. 19, 2013), http://boingboing.net/2013/10/19/dick-cheney-feared-assassinati.html.

[24] Bruce Schneier, "Debating Full Disclosure," Schneier on Security (Jan. 23, 2007), https://www.schneier.com/blog/archives/2007/01/debating_full_d.html; Andy Ozment and Stuart E. Schechter, "Milk or Wine: Does Software Security Improve with Age?," Usenix Security 15 https://www.usenix.org/conference/15th-usenix-security-symposium/milk-or-wine-does-software-security-improve-age (accessed April 21, 2016).

Disclosure is often adversarial, with firms threatening researchers (including those retained by their customers) who examine their products for defects.[25] Security researchers counter that their attempts to bring concerns to firms is met with silence or denial, or worse, threats of legal action.[26]

A growing body of empirical research[27] adds mounting evidence to the case for disclosure on researchers' own terms, rather than those of the vendor.

d. Abuse of the Digital Millennium Copyright Act Is a Barrier to Disclosure.

In the last years of the previous millennium, Congress passed the Digital Millennium Copyright Act, including section 1201, the "anti-circumvention" provision. Several courts have ruled that Section 1201 prohibits the circumvention of technological measures that effectively control access to copyrighted works even if the circumvention is done for an otherwise lawful purpose, or one with no nexus to copyright infringement.[28] And while the statute contains an exception for "security testing," that exception is narrow and provides little protection in practice.[29]

Section 1201 has been used to threaten and prosecute security researchers who come forward with information about vulnerabilities. Significantly, researchers who discovered critical vulnerabilities in smart TVs were discouraged from coming forward with their revelations,[30] leaving their users in the dark about their own safety, and leaving the vulnerabilities intact to be exploited by unscrupulous parties, from malicious pranksters to organized criminals.

[25] Cory Doctorow, "Oracle's CSO Demands an End to Customers Checking Oracle Products for Defects," Boing Boing (Aug. 11, 2015), http://boingboing.net/2015/08/11/oracles-cso-demands-an-end-t.html.

[26] Cory Doctorow, "Michael Lynn's Controversial Cisco Security Presentation," Boing Boing (July 29, 2007), http://boingboing.net/2005/07/29/michael-lynns-contro.html.

[27] *See, e.g.*, Robert M. Brady, Ross J. Anderson, Robin C. Ball, "Murphy's Law, the Fitness of Evolving Species, and the Limits of Software Reliability," University of Cambridge Computer Laboratory Technical Report 471 (Sep. 1999), http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-471.pdf; Ross Anderson, "Open and Closed Systems are Equivalent (that is, in an ideal world)," http://www.cl.cam.ac.uk/~rja14/Papers/toulousebook.pdf (accessed April 21, 2016); Sam Ransbotham and Sabyasachi Mitra, "The Impact of Immediate Disclosure on Attack Diffusion and Volume," Tenth Workshop on Economics of Information Security (June 14, 2011), http://www.econinfosec.org/archive/weis2011/papers/The%20Impact%20of%20Immediate%20Disclosure%20on%20Attack%20Diffusion%20and%20.pdf.

[28] *See MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 950 (9th Cir. 2010).

[29] *See* Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights (October 2015), at 160 n. 1028 (the security testing exception "would not cover the full range of activities in question").

[30] Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Comments on Proposed Class 20: Jailbreaking – smart TVs, http://copyright.gov/1201/2015/comments-020615/.

e. Open Standards Bodies Should Require Participants To Pledge Not To Assert Section 1201 or Similar Claims Against Independent Security Testing.

The proposed rules require that MVPDs make information available to navigation devices and apps using a specification defined by "open standards bodies."

Standards bodies routinely require their members to give up some of their rights in law as a condition of participation. For example, the Blu-Ray Disc Association requires that its members license relevant patents to all comers on "reasonable, nondiscriminatory terms."[31] The World Wide Web Consortium requires that its members license relevant patents to all comers on a royalty-free basis.[32]

Similarly, to preserve competition and safeguard security research, the FCC should require that standards bodies wishing to qualify as a source of specifications for MVPD communication with navigation devices adopt a nonaggression covenant through which licensors promise not to use anti-circumvention law to interfere with security research. Qualifying standards bodies would require members and licensees of any intellectual property to adopt a binding covenant promising not to assert claims under 17 U.S.C. § 1201 or similar laws against any acts of research, publication, or disclosure of any security vulnerability in a device or application that receives multichannel video programming. Such a requirement would further the Commission's goal of protecting consumer safety and privacy in the context of video navigation devices.

Conclusion

EFF believes that competition in end-user hardware and software for receiving MVPD programming is important and achievable. The Commission should continue its careful focus on consumer protection while eliminating avenues of overt or covert MVPD control over the design and functionality of competitive devices.

Respectfully submitted,

Mitchell Stoltz
Lee Tien
Ernesto Falcon
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109

[31] Blu-Ray Disc Association, "Amended & Restated Bylaws of Blu-ray Disc Association," cl. 16, http://blu-raydisc.com/Assets/Downloadablefile/BDA_Bylaws_v2.4.pdf (accessed April 21, 2016).

[32] World Wide Web Consortium, "W3C Patent Policy" (Feb. 5, 2004), https://www.w3.org/Consortium/Patent-Policy-20040205/.