Computer & Communications Industry Association

Tech Advocacy Since 1972

‘UNLOCK THE BOX’: HOW TO ADDRESS OPPOSITION AND BOOST COMPETITION

Introduction

A robust market for third-party competitive navigation devices requires that those devices have access to the same content that is available on TV set-top boxes that consumers lease from a Multichannel Video Programming Distributor (MVPD). Artificial limitations on existing functions, such as limited channel lists or the inability to record TV programs, would result in customer dissatisfaction and rejection of competitive navigation devices in favor of devices provisioned directly from MVPDs. Third-party devices should not be expected to compete on an unlevel playing field.

Consumers’ objectives are simple: they want to be able to choose how they watch video content, be it on a smart TV set, streaming box, tablet, or even a smartphone. Furthermore, if consumers pay to receive a service, they should have access to all of the content to which they are legally entitled regardless of the device and user interface (UI) they personally choose.

The FCC’s “Unlock the Box” Notice of Proposed Rulemaking (NPRM) proposes a solution to give consumers real choice. It would standardize “three information flows” to enable a competitive navigation device to obtain access to content. A standard must be established in the United States to define how competitive navigation devices communicate with MVPDs. While the “three information flows” can use IP delivery – the same technology behind ”over-the-top” video (OTT) – the three information flows are also compatible with existing cable TV and satellite distribution systems that may not support IP delivery directly to the home.

The FCC plays a pivotal role in setting the rules of the road regarding what competitive devices can do with content. As discussed below, certification and digital certificates provide tools that the FCC can use to ensure that devices follow the rules. With content protection as described in the NPRM, plus certification and digital certificates, the “Unlock the Box” system provides a high level of security for content and assures that navigation devices comply with FCC rules.

Understanding the FCC’s Unlock the Box Proposal: Explaining “Three Information Flows”

The Unlock the Box rulemaking sets forth three information flows needed for a competitive navigation device to properly access content from an MVPD in a secure and authorized way. The FCC’s three proposed information flows are: (1) *Service Discovery*, (2) *Entitlement Information*, and (3) *Content Delivery*. MVPD-provided set-top boxes and “apps” already have access to this information; the rulemaking requires that this information be made available to devices that are not affiliated with the MVPD.

The *Service Discovery* flow consists of the information necessary to create a user experience that allows a consumer to see the selection of channels and programming available for viewing. This flow carries data that includes the list of TV channels and the programs on those channels, as well as all of the Video on Demand (VOD) content on the pay-TV operator’s system.

The *Entitlement Information* flow carries data that describes which channels, programs, and VOD items a subscriber is allowed to playback or record. Content received from *Service Discovery* can be filtered so the UI can present what the user is authorized to view.

The *Content Delivery* flow carries the data for playback or recording of the content found via *Service Discovery* and confirmed to be authorized through the *Entitlement Information*. The Content Delivery flow enables the competitive device to access content in the system and present it in its own UI.

Data in these three flows need not always be "flowing" down to the subscriber's home (as is the case in traditional broadcast systems). Rather, the flows are compatible with two-way systems requiring "ask & fetch" models in which the competitive device must make requests to the MVPD to retrieve the data.

How the MVPDs' Proprietary App Proposal Boxes Out Competition

In stark contrast to the approach in the NPRM, in June 2016, a coalition of MVPDs (i.e., the National Cable & Telecommunications Association [NCTA], AT&T, and Comcast) introduced an alternative "proposal" that is light in detail and heavy with loopholes, proposing that *only* MVPD-controlled proprietary HTML5 apps may deliver pay-TV services. Delivery would occur from the cloud to devices, presumably without the need for an additional box.[1] Because MVPDs already provide most of this functionality to mobile devices today, this proposal largely perpetuates the current non-competitive landscape.[2] Third-party devices should not be expected to compete on an unlevel playing field.

The proposed reliance on HTML5 features like Media Source Extensions (MSE) and Encrypted Media Extensions (EME) benefit MVPDs by allowing them strict control on playback of content. MVPDs' HTML5 apps can mediate delivery of the audio or video service, including limiting "trick play functionality," preventing recording, and controlling stream bandwidth, along with selecting from available digital rights management (DRM) schemes. These MVPD benefits, however, in turn limit a competitive device's abilities to make local recordings, use custom remote controls, or launch and play content without loading the complete MVPD application, including the program guide. Device manufacturers also would be limited in their abilities to differentiate their devices through innovations occurring outside of the browser like high performing, multi-featured, custom-skinned media players.[3]

The information provided on the proprietary app proposal's support for content search from a third-party UI also is highly restrictive and ambiguous. There is no indication of how VOD search would work when device manufacturers rely on their own sources for

1 The FCC's proposal also can be implemented without additional set-top boxes if the cable operator so chooses.

2 The proprietary app proposal does not seem entirely HTML5-based. NCTA alludes to an installed component that would come from an app store. Today, however, HTML5 apps alone generally do not need to be available from an app store as only a URL is needed at which to point a browser. This raises questions about the types of contractual obligations that an MVPD would place on a competitive device manufacturer to make an app available through its app store and/or to install the app directly onto its hardware. MVPDs have incentives and abilities to act against competitors' interests during any negotiations concerning the apps.

3 The proposal lacks details about how the DRM schemes that EME uses would work with non-two way solutions like satellite. The proposal makes passing reference to a fallback of using DTCP-IP, which is similar to the FCC's Unlock the Box proposal where an HTML5-based UI could be "bolted-on" by leveraging the DLNA VidiPath™ standard.

metadata. The proposal does not specify whether the HTML5 app would need to be running for the search to be performed. It is not clear whether search results would be returned to the third-party UI or only shown in the HTML5 app, from which playback or scheduled recording could be restricted. Even if search results are returned, the proposal restricts use of universal search capabilities to only supporting licensed commercial content when used in conjunction with a search against the MVPD app. For example, imagine that the user performs a universal search in conjunction with an MVPD app with results restricted to MVPD content plus some other commercially licensable content. Later, the user performs a universal search against all of the device's content, which includes YouTube, Vimeo, and user-generated content. It is not clear whether the proprietary app proposal would disallow a search history on the device because it shows results combined in one place. Nor is it evident how the app would know what is licensed commercially available content. The proposal also would require device manufacturers to agree to support contractual agreements or changes to default device behavior, but it provides few details.

Finally, while aspects of the HTML5 app proposal have merit, HTML5 itself is an inadequate replacement for a "native" application that would run on a media device such as a TV set or streaming media player. HTML5 also cannot run on all devices (as noted by Roku in a recent filing with the FCC). When HTML5 can run, the performance and features of HTML5 apps are not up to the same level as embedded applications found in media devices. Thus, the MVPD proposal would result in customer dissatisfaction and rejection of competitive navigation devices in favor of devices provisioned directly from MVPDs.

How the Proprietary App Proposal and "Unlock the Box" Can Coexist

The proprietary app proposal shares some beneficial technological elements with the NPRM approach, such as using common encryption to support different DRMs on different devices, allowing MVPDs to have some control over streaming to protect advertising revenue models, and using a method of secure content delivery satisfactory to content providers. The proposal also maps to the content delivery flow of the FCC's Unlock the Box proposal. However, there is no real reason for an MVPD app to restrict a device to only using the MVPD's proprietary UI. Allowing a third-party device to access service discovery and entitlement information would enable all three flows on a competitive and innovative basis, and it would provide an alternative to the MVPD proprietary app. If an API can support search of the MVPD app to return results to a third-party UI, then an API also should be able to receive and process such metadata and entitlement information.

To leverage beneficial components of the proprietary app proposal, HTML5 functionality associated with playback and that of the UI must be separated. MVPDs are familiar with this concept, which they have utilized with content providers. Custom Platform Extras, an openly available set of specifications describing how a content provider's HTML5-based app works for content playback with enhanced UI features, can be combined with a distributor's or retailer's HTML5 app that manages entitlement control and purchasing, using a set of mutually agreed upon protocols.[4]

4 The complexity in Custom Platform Extras may not even be necessary. The MVPD serves as both distributor and content provider to the device manufacturer. Thus, the MVPD is entirely in charge of both protection schemes and entitlement management.

For example, a shared environment could be established where:

- An MVPD's app controls UI for authentication, entitlement, VOD, and critical messaging.
- An MVPD's app maintains control over delivery of the video content.
- A device manufacturer's app creates the primary consumer facing UI, integrating the MVPD-provided functions for authentication, entitlement, and critical messaging.
- A device manufacturer's app provides the media player, including the player UI, to connect into the MVPD-controlled delivery of video content.

It would be relatively simple and quick to standardize a protocol to share the information needed by the device manufacturer to establish a relevant UI skin of the player and to pass UI control events to the MVPD streaming application. A protocol-based shared environment would not necessarily limit device manufacturers to using HTML5 for their own UIs, would not restrict their preferred players to be browser-based, and would allow control over local recording when entitled. The device then would be open to innovative competitive navigation solutions. Otherwise, the only user-initiated recording possible would be to the "cloud" on an entirely permissive basis by the MVPD, and it would be subject to playback and viewing restrictions, controls, and additional fees on a basis entirely discretionary with the MVPD. This would be a large step backward from present CableCARD operation and even from the VCR world of the 1980s and 1990s that preceded DVRs. These freedoms to record, enjoyed by consumers and upheld by courts, would be recaptured by content providers and MVPDs.

A Digital Certificate Can Unlock the Box While Protecting Stakeholder Interests

Today, web browsers use a "lock icon" to signal to users that they are viewing a "secure" website rather than an "imposter" site. The "lock icon" indicates that the website owner has acquired a *Digital Certificate* from a *Certificate Authority*. Sophisticated parties like content owners and average consumers trust this model today for activities from online shopping to banking. The FCC's Unlock the Box proposal includes the concept of a published "certificate" that would help to ensure that a device would abide by a specific set of rules. A *Digital Certificate* would verify that a competitive device has been tested to conform to rules based on the published certificate's promise to ensure the device's compliance.

By requiring that a device has received a *Digital Certificate*, the Commission could ensure that the competitive device is contractually bound to this set of rules and could uniquely identify the specific device implementation. Offending devices could be blocked or deactivated by properly identifying them in a secure manner (e.g., subject to standard due process procedures, the offending device could be subject to having its *Digital Certificate* revoked).

A *Digital Certificate* could be created to implement the "Unlock the Box" proposal as follows:

1. A manufacturer builds a competitive navigation device, or a software developer creates an app for use on a consumer device.
2. A manufacturer or software developer submits its device/app to a *Certifying Body* connected to the *Certificate Authority*.
3. A manufacturer/developer signs a contract agreeing to abide by the rules tied to the *Digital Certificate* or to face the associated enforcement mechanisms.
4. The device/app is tested for compliance with the rules and, after passing, is issued a *Digital Certificate*.
5. The device/app now securely can show it is compliant with the rules set out in the *Digital Certificate*.
6. The device/app connects to an MVPD's service implementing the three flows. The MVPD's service requests its *Digital Certificate* to verify compliance.
7. Once the MVPD's service verifies the validity of the *Digital Certificate*, it provides the three flows to the compliant device/app.
8. In the event that a device is alleged to violate the rules:
    a. The contract signed by the manufacturer/developer can be used as the basis for triggering enforcement action.
    b. An MVPD is only required to supply service and three flows to devices that provide a valid (and not revoked) *Digital Certificate*. This method provides a means of enforcement even if the manufacturer/developer is non-responsive to contractual methods of enforcement.

Opposition Arguments About "Unlock the Box" Can Be Addressed

Some have called into question whether the FCC's Unlock the Box proposal is too complicated or otherwise flawed. All of their arguments can be addressed.

Privacy - Some opponents claim that there are issues with enforcing privacy requirements for devices. Others question whether existing privacy laws applicable to competitive devices would protect consumers to the same extent as those applicable to MVPDs. While the Federal Trade Commission (FTC) and various state Attorneys General have already addressed these arguments, the *Digital Certificate* also can address privacy-related concerns. The contract associated with the *Digital Certificate* can require that the device provider comply with its published privacy policy. Violations of such policies could be addressed by the FTC or by relevant state authorities.

Advertising - Some opponents argue that manufacturers would alter advertising during TV programs. The *Digital Certificate* could prohibit replacement or obscuring of advertising in the course of program delivery to a subscriber. Clear mechanisms would exist to enable MVPDs to deny service delivery to devices that have been found to violate these contractual provisions.

Copyright and Security - Some opponents argue that competitive device solutions would not be able to properly secure content and that this can only be done by the MVPD providing a complete application of its own. From a technical standpoint, a properly implemented hardware security system would effectively protect the chain of security around content handling. Good security implementations do not rely on applications passably written to protect content. Rather, they protect content no matter what else is happening in the system. The *Robustness and Compliance Rules* associated with any *DRM* or *Link Protection* system, which map to the *Content Security System* outlined in the Unlock the Box proposal, ensure that implementations are of high enough quality to properly protect content.

Copyright and Programmer Contracts - Programmers and MVPDs argue that their contracts contain provisions that should be obeyed by navigation devices. Some provisions may be relatively straightforward, such as preserving channel placement, not obscuring advertising, and meeting security requirements. These issues can be addressed in the contract tied to the *Digital Certificate* or the *Content Security System*. However, MVPDs and programmers also claim that other requirements in those private contracts only can be implemented in MVPD-controlled navigation devices. Yet today, CableCARD-based navigation devices have not been required to incorporate any features or functionalities to respond to these requirements from private contracts. Because third parties are not parties to and lack access to programmers' private contracts, there should be no expectation that competitive navigation devices can or should have to follow those restrictions.

Conclusion

Concerns raised by "Unlock the Box" opponents can be addressed utilizing existing technologies and practices with respect to certification. Privacy, advertising, copyright and security issues can be remedied through a forward looking solution that preserves and promotes a competitive marketplace for consumers to access the content they have paid for.

A *Digital Certificate* tied to contractual language pertaining to advertising, channel number preservation, and privacy compliance can enable consumers to experience and benefit from innovative navigation devices. The *Digital Certificate* should be included in the FCC's rules to help assure the availability of retail navigation devices.