



Stephen Schultze
Associate Director, Center for Information Technology Policy
Princeton University

Sherrerd Hall, Room 304
Princeton, New Jersey 08544
609-258-2175
sjs@princeton.edu

Via Electronic Filing

July 26, 2012

Marlene H. Dortch
Secretary
Federal Communications Commission 445 Twelfth St., S.W.
Washington, DC 20554

Re:

Commercial Availability of Navigation Devices, CS Docket No. 97-80; Compatibility Between Cable Systems and Consumer Electronics Equipment, PP Docket No. 00-67; In the Matter of Basic Service Tier Encryption, Compatibility Between Cable Systems and Consumer Electronics Equipment, MB Docket 11-169.

Dear Ms. Dortch:

On July 25, 2012, the I met with the following members of the Media Bureau to discuss the Commission's basic tier encryption Notice of Proposed Rulemaking ("NPRM"): Bill Lake, Chief; Nancy Murphy, Associate Chief; Alison Neplokh, Chief Engineer; Steven Broeckert, Senior Deputy Chief, Policy Division, and Brendan Murray, Attorney Advisor.

I expanded upon some of the points in my recent Comments.¹ Specifically:

1. MVPD providers have genuine "service theft" concerns that are independent of "content control" considerations. The CableLabs certification regime harmfully leverages encryption and licensing from the service theft context into the content control context. This introduces artificial incompatibility within the home and has restricted the market for and functionality of third-party smart video devices for the past decade. MVPD proposals in the current docket threaten the same harms for basic tier cable because they presume a structurally indistinguishable encryption and licensing scheme.
2. "Content control" measures within the home have proven to be ineffective at deterring unauthorized redistributors, who continue to publish near-real-time MVPD content on the public Internet. On the other hand, enforcement strategies that seek out hubs of such activity have been more effective. Although some of these enforcement actions have originated within the US Government, they are not typically within the mandate of the FCC. Furthermore, the content and cable industries are increasingly collaborating on non-governmental approaches to addressing digital infringement.

¹ See, Stephen Schultze Comments, MB Dkt. No. 11-169, PP Dkt. No. 00-67, CS Dkt. No. 97-80 (July 12, 2012).

3. "Open" standards such as DLNA are only as open as their underlying encryption regimes. The DTCP-IP licensing regime is itself required to comply with the CableLabs content control restrictions and other license requirements when it is implemented in any CableLabs-certified device.
4. Other in-home encryption and licensing schemes, such as HDMI/HDCP, have been successful in stimulating a third-party market only for narrow classes of devices that are defined in their license agreements. This "permission to innovate" environment cannot be seen as comparable with a vibrant third-party market for smart video devices.
5. In-home encryption and licensing schemes categorically foreclose many functions of truly open third-party devices. These schemes are premised on controlling device functionality, whereas open-source software and hardware permits unconstrained innovation. Even open source devices that integrate CableCard components are ultimately limited by the certification regime that applies to those components—for instance, any copy-control flag other than "copy freely" will disable their ability to decode the content even for authorized uses. Furthermore, as I noted in my Comments, over-aggressive MVPD content protection flags extend this non-interoperability unpredictably to a variety of video content, including content that is not pay-per-view or video-on-demand programming.
6. Boxee's reference to a "comparable successor to ClearQAM"² is vague and seems to be a logical impossibility. An encrypted basic tier cannot achieve its goal of service theft prevention if it is "in the clear," and it cannot be meaningfully comparable to ClearQAM if it is not. This lack of specificity echoes the unclear language in Comcast's Comments regarding a "licensing path for integrating DTA technology into third-party devices."³ NCTA is similarly vague in its recent Comments about a process by which, "Cable Operators shall use commercially available security technology that is licensable on a non-discriminatory basis to manufacturers of such retail devices," which, "shall sunset on the third anniversary."⁴

In its September 2000 Order, the Commission ruled that Section 629 did not prohibit MVPDs from imposing "content protection" schemes as part of their device licensing regime.⁵ It did so on belief that this ruling would spur industry to, "promptly finalize negotiations in order to bring to fruition the goals established by Congress in Section 629." At the time, the Commission evidently did not recognize that in-home encryption and open devices are irreconcilable, and it erroneously concurred with industry assertions that content control is relevant to and consistent with rules permitting service theft prevention technologies. In any case, the record now demonstrates over a decade of industry regimes that prevent a vibrant third-party device market in favor of in-home encryption. CableCard, DCAM, Tru2Way, IEEE 1394 DTCP encryption—and now DTCP-IP or other IP-delivered encryption regimes—all represent a fundamentally flawed approach that has strayed far from the original signal security and service theft rules.

² See Boxee Comments, MB Dkt. No. 11-169, PP Dkt. No. 00-67 (July 18, 2012).

³ See Comcast Comments, MB Dkt. No. 11-169, PP Dkt. No. 00-67 (June 27, 2012).

⁴ See NCTA Comments, MB Dkt. No. 11-169, PP Dkt. No. 00-67 (June 27, 2012).

⁵ See Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices, 15 FCC Rcd. 18199 (2000) ("Further Notice of Proposed Rule Making and Declaratory Ruling"), ¶¶ 26-32.

Marlene H. Dortch
July 26, 2012
Page 3

I have also attached a copy of an Ars Technica article in which I comment on these issues.⁶

Sincerely,
/s/ Stephen Schultze
Stephen Schultze⁷

⁶ Timothy B. Lee, “How Big Cable killed the open set-top box—and what to do about it. Ars Technica (July 24, 2012).
<http://arstechnica.com/tech-policy/2012/07/how-big-cable-killed-the-open-set-top-box-and-what-to-do-about-it/>

⁷ The preceding comments are entirely my own, prepared in my capacity as an independent academic, and do not necessarily represent the opinion of Princeton University or any other party.

LAW & DISORDER / CIVILIZATION & DISCONTENTS

How Big Cable killed the open set-top box—and what to do about it

Researcher argues the FCC's set-top box strategy is doomed to failure.

by Timothy B. Lee - July 24 2012, 11:15am EDT

GOVERNMENT 111



Inserting a multichannel (M-CARD) CableCARD decryption device

Steve Garfield

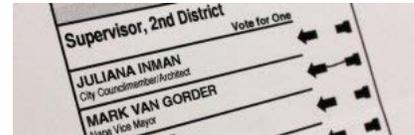
Steve Schultze once enjoyed the ability to record cable television content on the desktop computer in his Cambridge, MA home. But when he moved across the river to Boston, he was forced to switch to a digital cable service that encrypted most of its channels, greatly reducing the utility of his video recording gear.

Schultze, who now works for the Center for Information Technology Policy at Princeton University, writes that his experience is part of a broader trend. For more than a decade, the Federal Communications Commission (FCC) has tried to promote development of third-party set-top boxes—but poorly conceived strategy and cable company foot-dragging has largely foiled that agency.

A final nail in the open set-top box coffin could come soon. The FCC currently prohibits cable providers from encrypting basic cable channels in order to preserve compatibility with third-party devices. But these third-party devices have become increasingly rare, so the FCC is considering dropping the encryption ban altogether.

The cable industry opposes the ban, and it got a boost last month when set-top box manufacturer Boxee announced it had reached an agreement with Comcast that would provide Boxee products with access to encrypted Comcast content. The announcement was significant because Boxee had been a vocal supporter of the encryption ban.

TOP FEATURE STORY



FEATURE STORY (2 PAGES)

Saving throw: securing democracy with stats, spreadsheets, and 10-sided dice

"Risk-limiting audits" use sound math to make sure the right candidate won.

by Cyrus Farivar - July 24 2012, 8:00pm EDT

3

STAY IN THE KNOW WITH



LATEST NEWS



Apple vs. Samsung: hammering out details before a giant patent battle



Apple CEO Tim Cook: rumors are a "great thing about this country"



Craigslist sues site that makes its apartment listings easier to find (Updated)

TRUST EXERCISE

Google getting close to an antitrust settlement with the EU



Researchers control reactions between just two atoms

In a [recent FCC filing](#), Schultze argues that the FCC's whole approach to the set-top box issue has been misguided. Rather than regulating set-top boxes themselves, Schultze advocates freeing devices inside the home from the legal control of DRM vendors. He suggests that could be accomplished by requiring cable-supplied set-top boxes to provide an unencrypted video interface to third-party devices. Alternatively, in an interview conducted earlier this month, he told Ars that another solution would be to reform the Digital Millennium Copyright Act (DMCA) to allow the circumvention of DRM schemes.

A failed policy

In 1996, Congress ordered the FCC to establish rules to promote the development of third-party cable set-top boxes. The FCC followed instructions, issuing a series of regulations requiring the cable industry to develop standards that would enable third-party devices to interoperate with the incumbents' networks. TiVo, Boxee, Windows Media Center—let a thousand third-party video devices bloom!

But this approach had a basic problem: the companies developing the standards had a vested interest in seeing them fail. Cable incumbents prefer to have customers use their own proprietary set-top boxes. This gives them maximum control over the customer experience—and, as a consequence, maximum influence over the customer's wallet.

Unsurprisingly, the standards produced by this process haven't worked well. The first-generation standard, called CableCARD, included a DRM scheme that required device manufacturers to submit to a burdensome certification process run by CableLabs, a consortium of cable companies. Moreover, the original CableCARD specification supported only "one-way" communication; devices could receive video content, but they couldn't take advantage of interactive features offered by the cable companies' own set-top boxes.

Third-party devices based on the CableCARD [failed to catch on in the marketplace](#).

So prodded by the FCC, the cable industry began work on successor technologies that address the CableCARD's shortcomings. The industry developed Tru2Way as a complement to CableCARD technology that would allow third-party devices to access interactive services like digital program guides. Tru2Way was so cumbersome that it [never caught on](#). The most enthusiastic Tru2Way supporter, Panasonic, [abandoned the spec](#) in 2010.

On to attempt number three. The FCC is now developing a replacement for CableCARD called [AllVid](#). It enjoys the support of a [broad coalition](#) of software and consumer electronics companies—but (shock, awe) the cable industry is strongly opposed to the idea. And it's hard to imagine a workable standard will emerge from negotiations between the parties when the cable side of the table has every incentive to scuttle, hobble, or delay the project.

Control freaks

In his conversation with Ars, Steve Schultze pointed to the FCC's [Carterfone ruling](#), which opened the pre-breakup AT&T's telephone network to third-party devices in 1968, as a model for what the FCC is trying to do in the cable business.

"Unfortunately," he told me, "cable is a much more complicated technology than the phone system was or is. And so the cable companies have a lot more latitude to decide what they want to allow and what they want to prohibit."

Indeed, he said, dropping the ban on encrypting basic channels would be "the final step in this progression whereby the cable companies have leveraged their control over their networks and used encryption in particular as a way to dictate what can happen in the home." Boxee has conceded that point, he said, agreeing to give Comcast veto power over the design of Boxee's products in return for at least some access to video content.

Schultze said that cable providers have used the control provided by CableCARD to discourage the introduction of new devices. A number of devices, he said, had been "stuck in the certification queue." He speculated that when the FCC showed a renewed interest in the set-top box market a couple of years back, "CableLabs felt more pressure to certify devices. In the last couple of years, a couple of device manufacturers have made their way through the process."

Schultze also said CableLabs has forced manufacturers to limit device functionality. For example, "in order to be certified to the CableLabs regime you have to agree to respect a copy protection flag, even if the underlying content stream is unencrypted." As a result, he said, "CableLabs-certified devices often can't tune to some of the same channels that non-CableLabs-certified devices can."

Schultze believes that the FCC has been focusing on the wrong interface. Rather than restricting cable firms from encrypting content as it passes from the cable company to the customer's set-top box, Schultze believes cable companies should offer access to unencrypted video to devices inside the home.

"The provider's set-top box (or CableCARD) could still be responsible for decrypting signals in order to prevent service theft," he wrote, "but the video signal emitted from that device could be mandated to be 'in the clear' to any device that wishes to interoperate."

In the meantime, Schultze believes the current encryption ban "serves as a useful safety valve" to cable industry abuses.

Reforming the DMCA

Reforming the DMCA to allow reverse engineering would also address Schultze's concerns.

"The DMCA has foreclosed the development of open devices that decrypt the encrypted channels," he said. It has precluded uses that occur "against the wishes of the content owners but within the legally defined boundaries of accessible fair use and recording."

"If Congress invalidated the DMCA and we could crack HDCP, then it would be very easy for anyone to build a set-top box that just decodes that video signal coming out of the original set-top box," he said. "I think the HDMI port on the back of a set-top box is the closest thing we've got to an RJ-11 jack in the case of the Carterfone."

But, he noted, not all public interest groups agree with this position. Some of them, he said, have conceded the in-home encryption issue to push for the adoption of AllVid. As for Schultze, he worries this strategy is "just repeating the same problem we've had the whole time" because it "gives cable companies a hook on certification and content control."

READER COMMENTS 111



Timothy B. Lee / Timothy covers tech policy for Ars, with a particular focus on patent and copyright law, privacy, free speech, and open government. His writing has appeared in Slate, Reason, Wired, and the New York Times.
[@binarybits](#)

← OLDER STORY

NEWER STORY →

YOU MAY ALSO LIKE



A glimpse into the cutting edge of marine biology research



Why bother? The sad state of Office 2013 touch support



Paging Dr. Wasteland: One man's crusade to heal DayZ's zombie victims



Windows 8 GPU acceleration: good news for Metro



Dyad is an overwhelming audiovisual thrill ride



Get this—some ISPs provide faster download speeds than they promise



Spec Ops: The Line's lead writer on creating an un-heroic war story



First look: Excel 2013

SITE LINKS

[About Us](#)

MORE READING

[RSS Feeds](#)

CONDE NAST SITES

[Reddit](#)