

BEFORE THE  
**Federal Communications Commission**  
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
	)	
Comments:	)	GN Docket Nos. 09-47,
	)	09-51, 09-137
NBP Public Notice #27	)	CS Docket No. 97-80
Video Device Innovation	)	
	)	
	)	
	)	

**COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC**

## TABLE OF CONTENTS

SUMMARY AND BACKGROUND .....	4
DISCUSSION.....	4
A.    What technological and market-based limitations keep retail video devices from accessing all forms of video content that consumers want to watch?.....	8
B.    Would a retail market for network agnostic video devices spur broadband use and adoption and achieve Section 629’s goal of a competitive navigation device market for all MVPDs?.....	15
C.    Can the home broadband service model be adapted to allow video networks to connect and interact with home video network devices such as televisions, DVRs, and Home Theater PCs via a multimedia home networking standard?.....	19
(i) <i>If a “gateway” approach is being considered, does that mean that the entire effort regarding promotion of retail set top boxes in order to provide more choice and price competition for consumers is to be abandoned? .....</i>	<i>21</i>
(ii) <i>What would the capital cost be of developing and migrating to new MVPD set top boxes with the new “gateway”? Who would pay those costs? How long would a migration to those boxes take? How many consumers would even be interested in utilizing the gateway functions, and what would happen regarding consumer confusion with the hundreds of millions of analog television sets still in use? .....</i>	<i>22</i>
D.    What obstacles stand in the way of video convergence? .....	24

BEFORE THE  
**Federal Communications Commission**  
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
	)	
Comments:	)	GN Docket Nos. 09-47,
	)	09-51, 09-137
NBP Public Notice #27	)	CS Docket No. 97-80
Video Device Innovation	)	
	)	
	)	
	)	

**COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC**

Beyond Broadband Technology, LLC, (“BBT”) hereby submits the following comments in response to NBP Public Notice #27, which seeks input from the public on how the Commission can encourage the market for video devices that will assist the Commission’s development of a National Broadband Plan and serve the goals of Section 629 of the Communications Act.<sup>1</sup> BBT is the developer of a downloadable security solution (the “BBT Solution™”) that has been recognized by the Commission as compliant with current separable security requirement for video devices used by multichannel video programming distributors (“MVPDs”).<sup>2</sup>

---

<sup>1</sup> Public Notice, “*Comment Sought on Video Device Innovation*”, DA 09-2519 (rel. Dec. 3, 2009).

<sup>2</sup> Public Notice, “*Commission Reiterates That Downloadable Security Technology Satisfies the Commission’s Rules on Set-Top Boxes and Notes Beyond Broadband Technology’s Development of a Downloadable Security Solution*,” 22 FCC Rcd 244 (2007). See also *In the Matter of Comcast Corporation’s Request for Waiver of Section*

## SUMMARY AND BACKGROUND

When the Commission adopted its rules requiring separable security requirements for MVPD devices, it did so with the twin goals of establishing a retail market for, and of encouraging innovation in the development of, such devices. Even though the development of a retail market has lagged, the Commission has been more successful in fostering innovation than it realizes. Moreover, as described more fully herein, the innovation that has occurred and that will occur in the future – if the Commission continues to create the right environment – not only promises to finally fulfill the goal of encouraging a retail market for video-capable devices, it will do so with cross-platform solutions that will meet the Commission’s added and critically important goal of assisting the development of national broadband deployment and use.

## DISCUSSION

BBT informed the Commission three years ago that it had successfully developed a new, inexpensive methodology for allowing full security for video distribution on cable systems.<sup>3</sup> The BBTSolution™ also gives distributors maximum flexibility by enabling “downloadable” conditional access and any other

---

*76.1204(a)(1) of the Commission’s Rules*, Memorandum Opinion and Order, 22 FCC Rcd 228, ¶ 34 (2007) (indicating that an operator deploying BBT’s downloadable security solution would not need a waiver of the integration ban).

<sup>3</sup> Patents are now pending.

unique elements various competitors want to offer, such as alternative electronic program guides customized to individual subscriber preferences.

BBT developed this technology specifically to respond to the Commission's requirement that cable set top boxes have "separable security." The only separable security solution at the time was the CableCARD, which is the design used by the consumer electronics industry to offer a "common reliance" set top or integrated (in the television set, DVR, etc.) interface that can connect and work with all of the various cable television security and conditional access schemes currently employed.<sup>4</sup>

What was clear to BBT then, as now, is that the CableCARD technology is an expensive and inelegant method for achieving the Commission's ultimate goals. However, that does not mean that the requirement for separable security is flawed. In fact, by requiring separable security, the Commission set in motion efforts to design a new, far more robust and flexible technological solution for delivering video to consumers. That technology, at least in the form of the BBTSolution™ (as well, potentially, as some other downloadable security designs), is just now starting to enter the market. Moreover, as is explained in the "white paper"

---

<sup>4</sup> The BBTSolution™ approach respects the underlying desire of the consumer electronics industry to be able to build and sell a "common reliance" design. The BBTSolution™ secure microchip is backward compatible with the "common reliance" CableCARD form factor. A BBT CableCARD will be made available. Thus the consumer electronics industry has full flexibility to design and sell both CableCARD enabled "common reliance" devices as well as any new, innovative technology that they decide to market solely with alternate technologies. The consumer market is replete with such approaches, such as the CD/DVD/BluRay or AM/FM/HDradio devices now sold individually and in combinations nationwide.

attached hereto, the BBTSolution™ also promotes the Commission’s new goal of assisting the development of a national broadband plan, since it is platform agnostic – the same open standard downloadable security solution designed for cable (QAM) systems is equally applicable to broadband (IP) distribution, satellite (QPSK), or indeed, any other platform.

Specifically, as a result of BBT’s efforts, a cross-platform, inexpensive approach to establishing a secure communications channel between a consumer device and a distributor (whether a cable operator delivering aggregated channels or an individual server delivering video or data via IP on the Internet) is already in production in a secure microchip that can be employed in many form factors, from a “set-back box,” to a set-top box, to a USB or HDMI “dongle” that could be plugged into computers with current USB ports, or preexisting HDMI connectors (on a laptop, TiVo or television, for example) with the appropriate software. Of course, eventually such a chip could simply be integrated into consumer devices to assure a secure communications path while at the same time enabling “downloadability,” empowering wide ranging innovation. This is precisely what the Commission says it is seeking in this Public Notice. We believe it is already here.

Under the circumstances, it might be expected that BBT’s response to the Public Notice would be to suggest that a rulemaking be initiated immediately to

enshrine in law the attributes we have already designed. But BBT does not propose that approach. There are numerous complexities involved in developing new technologies. The last thing we need is technology engineered by lawyers. Rather, BBT supports those who call for a Notice of Inquiry to consider the evolution of video device technology and the video device marketplace. However, it would be an error for the Commission to suggest as part of that Inquiry either abandoning or substantially modifying the framework it created under Section 629. The fact that the Commission’s objectives with regard to video device innovation now include supporting the drive to broadband adoption and utilization in no way suggests that retrenchment from the separable security approach is warranted. Indeed, abandoning the commitment to separable security would undermine efforts to achieve the Commission’s goals just as – after delays that admittedly were longer than anyone anticipated – they are coming to fruition.<sup>5</sup>

The steps (and missteps) that have occurred along the route to achieving the Commission’s goals with regard to the video devices marketplace are such that even the language used by the Commission in trying to frame the questions to which it now seeks answers can create far more confusion and delay than would be the case if it simply allowed the current situation to evolve and mature. We

---

<sup>5</sup> While there are many proposals, from “network gateways” to “set back boxes” that can be explored in a Notice of Inquiry, the Commission should have no doubt that if such an NOI even suggests consideration of the substantial elimination of the “separable security” requirement, or if the Commission continues to entertain broad waivers of that requirement it will have the immediate effect of stifling the innovation that it has successfully fostered. The market will always revert to the status quo if given any reason to do so.

believe the Commission, if it fully applies the separable security rules, is already very close to achieving both its long held goal regarding the development of a retail market for innovative video devices and its newer, but essential goal of having that marketplace assist in the development of a national broadband plan. Applying the separable security requirement to all MVPDs, enforcing it, and possibly extending its scope to create a preference for cross-platform solutions should be sufficient to complete the process to which the Commission has devoted much time and effort.

With the preceding introductory comments in mind, BBT turns now to the specific questions posed by the Commission in the Public Notice. Our responses are structured to respond to each particular subject addressed.

**A. What technological and market-based limitations keep retail video devices from accessing all forms of video content that consumers want to watch?**

In the MVPD context, the initial limitation has always been that services such as “cable” television, “satellite” television, “telco” television, and the like do not all use a common platform like IP broadband. The various MVPD systems that deliver video programming to the public were built using different technologies with different capacities, security systems and business plans. Trying to now harmonize those differences is inherently difficult, and of questionable benefit. Some cable systems are one-way systems, but many are two-way today. Signals

are delivered in both analog and digital formats to varying degrees. Satellite distribution is done solely on a one-way platform, as is broadcasting. All have differing reception and tuning requirements.

The most significant obstacle to the development of a cross-platform retail device is incompatibility in security systems. The different MVPD distribution modes (cable, satellite, broadcast) will always require different reception and tuning capabilities because of their inherent technical differences. However, the dominant companies developing set top boxes designed different, closed, proprietary hardware security systems as well.<sup>6</sup> The challenge is to design a cross-platform system that both provides security and encourages maximum flexibility and innovation in the development of retail devices. Like a bus and a taxi supply similar, yet different services, MVPD distribution and Internet use should not be approached as if they are (or should somehow become) one and the same. It is essential that the Commission acknowledge this fundamental fact and work with (not against) it.

However, while traditional video distribution platforms and the Internet are and will continue to be different, they share core attributes that can provide the basis for the development and retail distribution of devices that can utilize both

---

<sup>6</sup> Securing intellectual property content is essential in both the cable and Internet context. While “DRM” (digital rights management) or some other form of software-based conditional access is additive, downloadable and useful, it is also true that “...there is a new crop of 18 (now maybe 13) year-old hackers every year”! There is general consensus among encryption experts that high-level security requires secure hardware implementation at both the sending and receiving end of a secure communications path.

infrastructures and thus help promote the objectives the Commission has articulated as well as expand the options of consumers. BBT believes an open, downloadable security solution allowing for the modular addition of conditional access, DRM, etc. is the best, and least restrictive approach to emancipating the retail device market, as well as for promoting cross-platform navigation.

Distribution of high value video programming on the Internet requires that same flexible security solution.

From a market perspective, the fact that the broadband IP distribution infrastructure has always been uniform and the MVPD infrastructure has not, answers the question of why the latter has been characterized by myriad devices and the former with only a few.<sup>7</sup> Changing the MVPD paradigm requires the development of a new security technology that is flexible enough to satisfy varying needs for security and authentication, that works cross-platform, that can be incorporated in multiple form factors (embedded in the set, the set-top, the set-back, a USB or HDMI dongle, etc.,) and that is “open” in that it is made available to all who want to use it at a uniform price and with specifications<sup>8</sup> for use that do

---

<sup>7</sup> The Commission’s list of “Internet devices” including such things as printers, refrigerators, game consoles and the like is not an apt comparison or example. The Internet delivers data used in many forms. MVPDs, as the name specifies, deliver video. There are hundreds of consumer choices for television sets, DVRs, VCRs, etc., all of which can be used to view or record video delivered by an MVPD. Enhanced retail availability of set top boxes would not alter the underlying difference between the two technologies. The challenge is to create consumer devices that will easily work with both.

<sup>8</sup> While specifications for use of such a device will be publicly available, implementation of security aspects will still require NDAs (non-disclosure agreements) for obvious security reasons. Those NDAs do not in any way inhibit

not impose any significant restrictions on innovation or competition. Creating and maintaining an environment in which such an approach can evolve and mature should be the Commission's principal goal.

For example, to date, one of the biggest market/technical impediments in creating such a security approach has been that some MVPDs, for market or technical reasons, use one-way distribution technology and others use two-way technology. The tendency has been to try to only design a satisfactory new separable security system device to work two-way. This would put smaller and mid-sized cable operators, for instance, in the position of having to make capital expenditures for equipment that is not cost effective for their purposes. They do not offer VOD, and their customers should not have to pay for equipment that is not utilized. Similarly, other infrastructures, such as DBS, and the additional multicast channels that may be offered by local broadcasters, have no technical way to use such two-way devices.

While the one-way/two-way divide has presented an obstacle in the past, the Commission's requirement for separable security has now encouraged the development of at least one system that does not require a two-way

---

the open development of consumer products using the BBTSolution™ nor do they impose any restrictions other than preventing the disclosure of confidential security details.

implementation. That was one of the primary first design goals adopted by BBT.<sup>9</sup> The BBTSolution™ can be implemented in both one-way and two-way devices.<sup>10</sup>

A second major technical/business impediment to the development of a uniform (downloadable) security solution has been that almost all such security approaches use a security design (Public/Private Key) that requires a single “trusted authority.” In other words, someone has to have control and knowledge of the authorized “private” keys used in the encryption and authorization system. Put bluntly, most companies do not trust each other enough to “trust” a “trusted authority.” There are also technical vulnerabilities with the “trusted authority” approach, but we need not delve too far into them, since from a business point of view it would appear that this approach, requiring the aggregation of confidential information, is simply not one that companies with large, proprietary customer bases are willing to seriously consider. Again, solutions have been found to this problem precisely because the Commission’s separable security mandate is

---

<sup>9</sup> BBT’s founders are all operators of small cable systems. The CEO/CTO, Bill Bauer, was the Chair of the original committee at CableLabs responsible for designing what ultimately became the DOCSIS modem. The Commission has favorably cited DOCSIS as a successful model for the efforts being explored here. BBT has always emulated and promoted that model for the development of the BBTSolution™. The underlying idea is that if the technology is elegant and simple enough to work with the most restricted technical options, such as one-way transmissions, it will *ipso facto* then be capable of modular improvements and enhancements for the more technically advanced, and future systems.

<sup>10</sup> Contrary to assertions that some parties have made to the Commission in the past, a separable security requirement can be applied in both one-way and two-way environments without significant economic disparities. The BBTSolution™ works in both environments. It does not require embedded two-way communications capability.

fostering creative innovation. The BBTSolution™ downloadable security approach does not require a “trusted authority.”

One clarification is necessary at this point in responding to the questions posed in the Public Notice: there is a fundamental difference between “Internet Access” and what an “MVPD” does. Comparing the two is not terribly useful. All of the multitude of interactive Internet devices cited by the Commission relate to a communication where the consumer seeks out a specific speaker, aggregator, or data source. All of that data is then available (either free or for a fee or secured in some way) to authorized users. An MVPD video content distributor sells a package of programming and information that is essentially “streamed” at all times (unlike the Internet data) to the user.

These are inherently different technologies. Internet access is totally “on demand,” while MVPD service is far more efficient at sending things like High Definition television pictures to a large segment of the population at the same time. If the Internet infrastructure was tasked to deliver all the HD programming that is watched on an average prime-time evening it would collapse. It is simply not efficient enough nor does it have sufficient bandwidth to do so at this time.

For the very reason that these different structures are employed so differently, the interfaces also are inherently different. A television set is not a computer. While there may be some “convergence,” the fundamental uses are

different. Someone who is solely interested in “watching television” should not have to pay for a unified device that includes a keyboard. A “computer monitor” is designed differently and has different capabilities than a “television set.” Thus it is a mistake to try to make them all work alike. The technical and market-based differences are real and legitimate.

The Commission’s focus should be on how these technologies can be made to work together at the most basic, primary level by establishing a secure communications path, whether on cable, satellite, broadband, broadcast etc. The market, and the differences in the segments of the market, would then be free to flourish with offerings geared to all of the variable desires of consumers. To do otherwise would stifle, not encourage technology development and adoption.

It is precisely because of confusion and complexities like those just mentioned that BBT supports the issuance of a Notice of Inquiry by the Commission to explore these issues. But it is premature to consider establishing “standards” when it is not yet clear what is needed, or what is now becoming available as a result of the innovation-promoting framework the Commission already has put in place.

**B. Would a retail market for network agnostic video devices spur broadband use and adoption and achieve Section 629's goal of a competitive navigation device market for all MVPDs?**

There are two assumptions intertwined in the Public Notice's query regarding "network agnostic" devices. First is the question of whether there is or can be a device that is "agnostic" regarding the various technologies; second is the question of developing a "standard" to achieve such a device.

There is nothing preventing a device manufacturer from creating a set top box or even an integrated television set today that has a DTV, cable and DBS tuner as well as an Internet modem built into it. All of those individual network tuning devices are commercially available right now along with the hardware and software needed for the device to "talk" to the networks. Such a device would be "network agnostic." But it would be prevented from working in a "converged" manner because of the various incompatible security schemes. It is not network tuning or navigating that prevents the development of an "agnostic" device; it is the security schemes and cost.

In the discussion above, we have already explored whether there are technical answers to the underlying issue of establishing a secure communications path. There are, and it can be network agnostic. The Commission's primary – indeed, only – objective should be to create and maintain an environment in which the technical means for establishing, authenticating and securing the

communications path can mature and evolve. Provided that the means by which a secure communications path is established allows for maximum flexibility with respect to downloadable conditional access, DRM, “Tru2way”, EPGs, alternative navigation, etc., everything else should be left to the marketplace. The complexities of trying to deal with and “standardize” not only all of those variables, but also the technical advances sure to come, would make such an effort unlikely to succeed.

Much like the market for a combination fax/scanner/printer/copier, there will be a certain segment of consumers interested in having one device that does everything – but just a segment. More likely, there will be greater demand for a variety of devices that possibly accept connections from both the Internet and an MVPD but only do certain things with those connections; for instance, allowing for viewing, as on a television screen, from alternate networks, but not necessarily using a keyboard for Internet access, leaving that to another device such as a computer. Some other devices may be used for both watching video and navigating the Internet. Specialized devices may just access specific “channels” on the Internet but not navigate through user-entered URLs, while others might be designed solely for downloading and storing, like a DVR. The possibilities are endless and it is neither possible nor appropriate for the Commission to try to anticipate them all, or worse, set standards for them. Such a ubiquitous “standards”

approach would most definitely inhibit both broadband and MVPD growth and innovation.

We urge the Commission to look at these issues with simplicity and modularity in mind. Identify the primary common denominator needed to allow all of the above devices to be deployed across all platforms, spur its development, and then allow the marketplace to operate. We believe open standard downloadable security is that primary common denominator. If the Commission stays true to its current requirement of separable security and applies it across all MVPD platforms, an open standard downloadable security approach, such as BBT's or some other, will shortly emerge as a neutral mechanism that will allow all of the innovation and broadband adoption that the Commission is seeking. No new standards are necessary – just continued adherence to the already existing requirement for separable security will accomplish the goal. Overly-broad exception to that requirement for DBS or IPTV systems or for “low cost” boxes will unquestionably nullify the development and adoption of the new technologies that are now emerging and that will accomplish virtually all of the Commission's stated objectives for technological innovation, retail market development, and broadband deployment.<sup>11</sup>

---

<sup>11</sup> BBT is painfully cognizant of the allure of “small system” low-cost set top box waivers for limited functionality boxes. However those waivers serve neither the operator nor the consumer. They significantly reduce the potential initial market for new technology, slowing or stopping development. Smaller systems constitute the initial market for most new technical innovations, because larger operators have inherent transition problems caused by their

The benefits of an open standard downloadable security approach such as the one designed by BBT go beyond assisting in the development of a retail market for MVPD devices. That will happen because downloadable security is a technologically superior, more flexible and less expensive approach to separable security than CableCARDS. It is also backward compatible with CableCARDS, thus protecting the embedded base of retail devices that use that technology, thereby continuing to support the consumer electronics industry’s “common reliance” device that it says it wants to market.

Equally important is the fact that an open standard downloadable security approach that is platform agnostic can be used in multiple form factors which will allow, for instance, MVPD operators to offer their aggregated channels for delivery on the Internet (the “TV Everywhere” concept) with full security and authentication using the same devices (embedded in a set top, a television set, a USB or HDMI dongle, etc.) that can also be used to retrieve other secure communications such as medical health records or other confidential materials on the Internet. The “value” applications of a network agnostic secure

---

embedded proprietary base. The new technology, spurred by adherence to the Commission’s existing rules, unlike the low-cost waiver boxes, will also allow small operators to compete with all digital, MPEG4/2 full HD delivery and expanded broadband bandwidth, all of which aids the consumer and the Commission’s broadband goals. That this new technology innovation can now also play a significant role in Internet secure communications confirms the Commission’s approach to spurring innovation, so long as it continues to adhere to it.

communications path are endless. Adoption follows perceived value. That, as we understand it, is the Commission's objective.

**C. Can the home broadband service model be adapted to allow video networks to connect and interact with home video network devices such as televisions, DVRs, and Home Theater PCs via a multimedia home networking standard?**

It is not clear how a home media networking standard, as mentioned in the Public Notice, would aid in accomplishing the stated goals of the Commission. Home networking has been governed by voluntary standards that were initiated in 2004 (in the case of DLNA). Adhering to the standards cited by the Commission is only relevant to those consumers who desire to transport, manipulate or transfer video signals from one compliant device to another in the home. Well over 5000 consumer devices are already compliant with the standard, yet there is no indication that it has gained majority consumer acceptance or use.

A "gateway" required to include MVPD signals would not instantly provide consumers with some form of seamless access and ability to manipulate individual video services from various platforms unless all platforms, and more importantly the services delivered over them, also were required to be uniform. In other words, video would have to be delivered in an "IP" form, or "IP" would have to be delivered in a standard (such as HDMI) format. If HDMI was the "standard" chosen for the "gateway," then all broadband deliverers would conversely have to create specialized "gateways" since MVPDs are effectively already required to

deliver their digital HD signals through a uniform HDMI “gateway.” To add to the complications, there would have to be some form of mandate that all of the contracts MVPD providers have with programmers would have to be changed to allow for individual manipulation and use, rather than the current model which in almost all cases requires delivery in an aggregated form.

The technical complexities of the “gateway” approach are explored in some detail in a petition for rulemaking recently submitted to the Commission.<sup>12</sup> That petition provides an excellent discussion of standard setting, but does not deal at all with the financial, business, or market aspects of the “gateway” concept. It only explores one potential technical approach to the issue: essentially requiring all MVPDs to supply a video “gateway” that delivered video signals in IP. Any formal standards-setting body effort, as described by the Petitioners, to establish such a technical approach would take years to complete.

The suggestion that the Commission is in a position at this time to “require a standards-based gateway” is, we believe, proved inaccurate by the very comprehensive discussion in the Petition and by the questions posed here by the

---

<sup>12</sup> Petition for Rulemaking of Public Knowledge, Free Press, Media Access Project, Consumers Union, CCTV Center for Media & Democracy, Open Technology Initiative of New America Foundation, RM \_\_\_\_ (filed Dec. 18, 2009). Petitioners “ask that the Commission (1) combine all open proceedings relating to cable set-top box commercial availability and device interoperability, (2) freeze all separable security waiver requests until the rules are updated, and (3) issue a Notice of Proposed Rulemaking to require a standards-based gateway for accessing the video services of all multichannel video programming distributors, or MVPDs.”

Commission.<sup>13</sup> Prior to any substantive response to questions about the “pros and cons” of a specific pre-existing home networking standard, or some new “gateway,” there are some far more fundamental questions which must be addressed:

- (i) *If a “gateway” approach is being considered, does that mean that the entire effort regarding promotion of retail set top boxes in order to provide more choice and price competition for consumers is to be abandoned?*

A “gateway” is simply another term for a set top, or set back box owned, controlled and required, under this scenario, to be supplied by the MVPD with a mandated technical output and defined set of capabilities. The “gateway” aspect, in whatever technical form was ultimately chosen, combined with the proprietary pre-existing set top box designs for tuning, security, return path communication (if any) etc., would likely increase the cost of those boxes. It would freeze development and innovation for new MVPD set top devices. In other words, it would accomplish the exact opposite, with regard to those devices, of what was mandated by Congress in Section 629.

The interest in a “gateway” approach seems to be based on the theory that this would be a trade-off necessary for the development of other consumer devices that could benefit from having a uniform input from both MVPD and broadband

---

<sup>13</sup> There are several significant parts of the Public Knowledge et al. Petition that BBT can support. In particular, the suggestion that all of the various proceedings surrounding the issues being explored in the instant Public Notice be consolidated and the request that the existing rules be maintained and enforced pending the formal adoption of a new policy, are consistent with the views expressed herein.

suppliers. But what of all the consumers who may not have any interest in such “converged” use, especially if it means that consumers would be forced to purchase new, more expensive “converged use” devices? Alternatively, attempts may be made to rationalize the “gateway” concept as a necessary addition to the requirement for separable security. But if that is the case, then isn’t the market already responding to the perceived need, since, as already noted herein, downloadable security solutions are now appearing on the market and there are also video devices (such as Slingbox and TiVo) which incorporate both MVPD and broadband signals the way they are delivered today.

- (ii) *What would the capital cost be of developing and migrating to new MVPD set top boxes with the new “gateway”? Who would pay those costs? How long would a migration to those boxes take? How many consumers would even be interested in utilizing the gateway functions, and what would happen regarding consumer confusion with the hundreds of millions of analog television sets still in use?*

The questions posed above are just the tip of the iceberg and are recited simply to illustrate that much more thought and analysis of the “gateway” concept is needed before the Commission can decide whether to propose specific rules and standards in a formal proceeding. The only appropriate step the Commission should take with regard to this very broad concept would be to have a Notice of Inquiry to explore the numerous technical and market questions such an idea raises.

One last point should be made at this juncture. If one of the Commission's objectives is to promote broadband use, and there are now technologies and markets developing (such as "TV Everywhere", Hulu, etc.) for the distribution of almost all forms of video content (including the channels offered by MVPDs) in "IP" form on the Internet, then why is there any concern about forcing a technical convergence of MVPD and broadband delivered signals? As already explained herein, new technical innovations have been developed, specifically with a platform-agnostic open standard downloadable security solution, that will allow all the video product the Commission is concerned about to easily be delivered to consumers in whatever form they wish to utilize.

The legal, contractual and market decisions of intellectual property owners will ultimately determine which of their products is available in what form regardless of technical requirements. So long as the Commission maintains its current course and enforces its rules, it would seem that the market is already addressing the issue of consumers who wish to access those video products on today's IP enabled devices. The proposed "solution" of a mandated uniform "gateway" for all MVPDs using a singular, anointed protocol can only have the

effect of freezing any new development. Why? Once again, we caution against “engineering by lawyers.”<sup>14</sup>

**D. What obstacles stand in the way of video convergence?**

The Commission’s summary in this portion of the Public Notice is entirely accurate but confusing in that it attempts to equate broadband and MVPD navigation devices. As noted above, broadband and MVPD devices do different things. One selects individual sources and data (in video or other form) which is then initiated and sent from a server. The other “dips” into a pre-existing aggregated stream of video programming. In the MVPD context, it is the video program package that is sold to the customer. In the Internet context, what is being sold is connectivity. While the consumer video experience of viewing (whether on a computer or a television set) may be in some ways “converging,” the technologies are not. Only a formal regulatory intervention in the marketplace by the Commission could force such a technical convergence. And, as we have explained throughout, such an all-encompassing intervention would likely be destined to fail.

The technologies used to deliver various forms of video or data are different and always will be. While there is some surface similarity, in the

---

<sup>14</sup> In the same vein, the Commission’s requirement for a “1394 – Firewire” connector did absolutely nothing to advance the development of a retail set top box (indeed, it inhibits that development by adding very high costs for very limited use). If anything, a substitution of, optionally, an Ethernet or USB port for the current 1394 requirement would make far more sense and promote more innovation.

consumer use of VOD, for instance, the infrastructure challenges are different. IP is universal on broadband. MVPDs use entirely different modulation schemes from QAM to VSB to QPSK. Those schemes are serviced by vast embedded bases of consumer tuning/security/authentication devices. They are not going to be replaced any time soon.

A “network interface solution” will not change the fundamental differences and requirements of the navigation devices, such as the need for tuners for differing modulation schemes. Consumers can already navigate all of the varying sources of video content. The Commission’s underlying question seems to be what can be done to simplify, to the degree possible, the navigation of those multiple sources (understanding that the tuning, manipulation of modulation schemes, etc., are not likely to be technically unified) while at the same time encouraging innovation and competition in the retail market for MVPD video navigation devices, and additionally, promoting the adoption of broadband.

We have identified the biggest impediment as proprietary security. The Commission also reached the same conclusion and already has a rule requiring “separable security” which we have shown is now promoting significant innovation in new security designs for such navigation devices. These innovative new security designs have the potential to significantly alter constraints on the distribution of intellectual property and confidential information by MVPDs and

on the Internet. The biggest obstacle to encouraging that innovation should not be the Commission itself.

By creating major exceptions to the rule requiring separable security, exempting all MVPD distributors other than cable, and creating the impression that it will grant numerous requests for “low cost” limited functionality set top boxes, the Commission has undermined the potential market it was trying to forge for the development of new technology for separable security set top or integrated devices. As the famous comment from the cartoon Pogo said: “We have met the enemy, and they is us!”

There are very few who will argue that the current enforcement of the existing rules makes any sense, particularly applying those rules to only one MVPD competitor. A true, open standard downloadable security solution is ready for distribution. It resolves the reluctance of operators to share confidential information by not requiring a “trusted authority.” It is operable on both one-way and two-way technologies, and it is platform (network) agnostic.

We are not here proposing that the BBTSolution™ be adopted as a “standard.” The standard-setting process is long, political and arduous. The marketplace, we believe, will be far more nimble in choosing our, or another downloadable security solution once it is clear that the Commission intends to enforce the rules it has already adopted. The concern about incompatible delivery

methods and the speed of innovation is likewise resolved by adopting a downloadable solution that allows total flexibility both now and in the future. By simply recognizing that the essential primary common denominator is the need for a secure communications path and then ensuring an environment where it can flourish and mature through innovation and competition, the Commission is more likely than in any other way to achieve its goals.

Respectfully submitted,

**BEYOND BROADBAND TECHNOLOGY, LLC**

/s/ 

William D. Bauer, CEO/CTO  
Beyond Broadband Technology, LLC  
1140 10<sup>th</sup> St.  
Gearing, NE 69341

Stephen R. Effros  
Effros Communications  
PO Box 8  
Clifton, VA 20124  
steve@bbtsolution.com  
703-631-2099

December 22, 2009

*A "WHITE PAPER" ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION*

*Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system (OSDS™) which does not require the use of a "trusted authority". The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.*

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This "White Paper" is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

## INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about "information security," it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is "downloadable," security conditions can be changed repeatedly, depending on the use. In other words it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB "dongle") for instance, could securely access multiple video programmers via the Internet, each with it's own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

## THE BASICS

The BBTSolution has two parts; a secure microchip in the receiving device, and an "HSM" (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information on the Internet, for instance. HSM's could also be integrated into

devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. The cost of the HSM enabled equipment will vary depending on the use. The current design for cable television systems, including the computer, costs less than \$10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that the basic Hardware Security Module enabled for use on computer servers can cost half that, or even less.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a “thumb drive” or “dongle”) that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Micro, are inexpensive (they are currently priced at \$5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known “Dolby™” system is included in most consumer audio devices today.

## BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBTSolution is that the receiving device, such as a television set, need not be a “two-way” device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBTSolution device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

## THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for “separable security” for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner, and descrambler) that had “integrated security”. That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or “conditional access” systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the “conditional access” components of the system. Unfortunately, CableCARDS are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers

today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, “backward compatible” with CableCARDS.

One of the original objectives of BBT was to design a new “separable security” system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman’s language used to describe these systems, which was subsequently adopted by the FCC, was “downloadable conditional access systems” or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption /decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

## A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A “TRUSTED AUTHORITY”

The traditional approach to establishing a secure communications path is to use a “public/private encryption key” dialog between devices. However this standard approach also requires that the “private key” be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a “trusted authority” holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a “trusted authority,” thus eliminating the two most significant drawbacks of the traditional approach.

With the BBTSolution, the “public/private” keys that enable devices to securely communicate are replaced by a “symmetrical key” approach. Keys are derived internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a “trusted authority” and the risk factor of “hacked” or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the “threat target” for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term “conditional access,” the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

## DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include “conditional access” protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus the BBTSolution has been designed in an “open” format where specifications will be made available so that anyone can design “conditional access” software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as rigorous as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB “stick”, which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized “conditional access”

protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be authorized only with thumb print verification as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a “virtual machine” or “tool box” that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12<sup>th</sup> power combination of encryption/decryption processes. However one can never assume that something simply can never be “broken,” so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a “software-only (DRM--”digital rights management”) approach to encryption or conditional access is subject to constant challenge. As the saying goes, “..there's a new crop of 18-year-old hackers every year!” The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional “DRM” chosen by the information provider, the ability to “download” protocols allows for other flexibility as well. For instance information stored in different formats may require that a “reader” be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

## CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a “trusted authority” and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet , in particular, can fundamentally change the way those platforms are used today.

12 08 09

Contact: Steve Effros

steve@bbtsolution.com

703-631-2099