Downloadable Security Technology Advisory Committee
Federal Communications Commission

Summary of Meeting
February 23, 2015

The Federal Communications Commission's Downloadable Security Technology Advisory Committee (DSTAC) was convened for its annual meeting at 10:00 A.M EST on February 23, 2015 at the Federal Communications Commission. A full video transcript of the meeting is available at the FCC website at http://www.fcc.gov/DSTAC.

In accordance with Public Law 92-463, the entire meeting was open to the public.

Committee Members Present:

Dr. Ahmad Ansari, Director of New Product Development, AT&T (via telephone)	**John McCoskey,** Executive Vice President and Chief Technology Officer, Motion Picture Association of America
Brant Candelore, Senior Staff Member, Adv. Development Group, User Experience Technology Center, Sony Electronics Inc. (via telephone)	**Bruce McClelland**, President of Network and Cloud & Global Services, ARRIS (via telephone)
John Card II, Director of Standards and Technology for EchoStar Technologies, LLC (representing DISH Network)	**Milo Medin**, Vice President of Access Services, Google, Inc.
Matthew Clark, Principal, Business Development Digital Products, Amazon, Inc. (via telephone)	**Alan Messer**, Vice President, Advanced Technology, Samsung Research America, Inc. (via telephone)
Bob Clyne, Senior Vice President of Engineering and New Technologies, Cablevision Systems Corporation	**Jay Rolls**, Senior Vice President and Chief Technology Officer, Charter Communications, Inc.
Adam Goldberg, Principal, AGP, LLC (representing Public Knowledge)	**Dr. Simha Sethumadhavan**, Associate Professor of Computer Science, Columbia University (Special Government Employee) (via telephone)
Mark Hess, Senior Vice President, Office of the Chief Technology Officer, Business and Industry Affairs, Comcast Corporation	**Brent Smith**, President & Chief Technology Officer, Evolution Digital
	Cheryl Tritt, Senior Counsel, Wilkinson, Barker, Knauer LLP (Committee Chair)
Brad Love, Chief Technologist, Hauppauge	**Dr. Joseph Weber**, Chief Technology Officer, Service Provider Business Unit, TiVo, Inc.
Kenneth Lowe, Vice President and Co-Founder, VIZIO, Inc.	**Robin Wilson**, Vice President, Business Development, Nagra

FCC staff attending: **Scott Jordan**, Chief Technology Officer; **William Lake**, Chief, Media Bureau; **Nancy Murphy**, Associate Bureau Chief, Media Bureau, Alternate Designated Federal Officer; **Brendan Murray**, Assistant Division Chief, Media Bureau, Policy Division, Designated Federal Officer; **Alison**

Neplokh, Chief Engineer, Media Bureau; **Paula Silberthau**, Attorney-Advisory, Office of the General Counsel.

Chairperson Cheryl Tritt began the meeting by welcoming the attendees to Washington and taking roll. Media Bureau Chief Bill Lake then thanked the committee and expressed that the committee's work will be positive for consumers, operators, and electronics manufacturers. Chair Tritt introduced herself and summarized the topic set forth in Section 106(d) of the STELA Reauthorization Act of 2014.

Scope of the Report

Alison Neplokh, Chief Engineer of the Media Bureau, began the discussion regarding the scope of the report that the advisory committee will produce. She listed use cases of the types of devices and services that would rely on a downloadable security solution, sought comment on the inputs and outputs of a downloadable security system, and asked for other issues that the committee will need to consider as it drafts its report.

John Card II explained that the direct broadcast satellite ("DBS") industry is set up differently from other multichannel video service providers ("MVPDs") because their systems must assume that the communication is one-way from the provider to the subscriber.

Jay Rolls raised the issue of renewability. He said that it is necessary for adequately protecting high quality content, like ultra-HD.

Mark Hess asked Ms. Neplokh to verify that her suggestion is that the solution should be hardware-based. Ms. Neplokh clarified that she used the term "black box" as a metaphor rather than to refer to a piece of hardware. Mr. Hess said that just like DBS, cable systems often rely on one-way broadcast communication, and that it would be very helpful for the committee to educate one another about how their systems work.

Adam Goldberg said that from a consumer perspective, it is important to remove the specifics of the delivery network from the equation, to allow consumers to buy a box, plug it in, and have it work with the service to which he or she subscribes.

Milo Medin said that the committee needs to think short-term and long-term, and realize that companies are transitioning at different speeds. Mr. Medin said that some companies have already or will very soon transition to full Internet Protocol ("IP") delivery, but others may take a long time to make that transition, and the committee should develop a solution that bridges that gap. Mr. Card and Mr. Rolls agreed that operators are on very different time schedules, but that IP will be involved somehow (particularly with respect to sending video inside a subscriber's home).

Joe Weber said that it is important to have one downloadable security system (or few) because it is difficult for manufacturers to build to many different systems. Mr. Rolls agreed that this was a key question, and that it may be difficult because there are many different existing transport systems and security systems. Bob Clyne stated that MVPDs have a reciprocal need that consumer devices work with all of their services.

Alan Messer stated that he did not like the idea of assuming that this downloadable security system would require a chip. Mr. Goldberg agreed. Robin Wilson added that there is a range of security protections, and the strength of the security that the content owner requires increases commensurate with the value that the owner puts on the content.

Brent Smith said that one of the problems with the legacy regime is separating security from MVPD service. He said that MVPDs do not manage new over-the-top services that run on mobile devices; that is, they do not control encryption, delivery, or the type of player used to view the service. Ahmad Ansari agreed, and said that AT&T provides applications and value added service in addition to audio and video. John McCoskey said that it is important to recognize that content is licensed to MVPDs individually—each license has different technical requirements—and that the solution needs to honor that. Ms. Neplokh said that the focus of the working group is to develop a downloadable security system to replace CableCARD.

Mr. Card raised the issue of how to treat over-the-top services. He relayed that in discussions with Commission staff, the preference is for the committee to make clear in its report whether it addresses those services or does not. Mr. Medin said that over-the-top services should fall outside the scope of the committee's work because those services are available on many devices. Mr. Goldberg said that if the committee can define a set of inputs into a device and if the service is IP-based, a lot of problems would go away. Mr. Hess said that over-the-top needs to be included, and asked whether the Commission intends for the committee to consider them when drafting the report. Brendan Murray clarified that the Commission would prefer that. Ms. Neplokh said that it may be difficult for the committee to foresee where that market and technology goes. Kenneth Lowe said that the committee should consider over-the-top providers, and Bruce McClelland agreed.

Outputs

Ms. Neplokh asked the group if it is possible to develop a solution that can provide the services necessary to have a platform and technology-agnostic system to let retail devices access MVPD services, and if so, what the inputs and outputs need to look like. Mr. Card responded that DBS does not have a static input, and DBS technology is complex and consistently evolving, so it probably would not be ideal to plug a device directly into a satellite dish. Mr. Goldberg said that a retail device would need information necessary to (i) discover available services, (ii) tune to those services, (iii) purchase additional services, (iv) provide other ancillary things like emergency alert information, closed caption, and parental control information, and (v) output audio and video. Dr. Weber agreed, and said that copy control information and encoding rules are also necessary, to allow for a consistent user experience. Mr. Card later disagreed with Dr. Weber, saying that MVPDs distinguish their services via different user experiences, and Dr. Weber later clarified that his call for consistency was limited to encoding limits.

Mr. Clyne asked what the specific tasks of the solution would be, and whether it would be expected to process audio and video, or simply decrypt and pass video back to the device. Ms. Neplokh indicated that the working groups could address that issue. Mr. Medin supported the approach of establishing basic functionality that a device should expect to have.

Mr. Hess stated that extra hardware would increase energy consumption and is unnecessary in an IP-based system. He also stated that his company's service is a complete, holistic, interactive service that cannot be divided, and asked Commission staff to clarify the term "service."

After a break, Ms. Neplokh directed the conversation to list inputs and outputs. She listed the same outputs that Mr. Goldberg and Dr. Weber listed (discovery, tuning, purchasing, ancillary services, video and audio, and copy control information). Brad Love stated that he would also like to add guide data to the list. Mr. Medin said that data should also include data for on-demand services. Mr. Card said that there should also be a service identification element that identifies the specific services that are available.

Mr. Rolls said that there are six elements of a conditional access system: (i) core ciphers, (ii) network transport, (iii) video codecs, (iv) system information (e.g., channel lineup, network configurations, program guide, etc.), (v) control channels, and (vi) middleware.

Mr. Card said that MVPDs have commercial requirements that may not jibe with the outputs of a conditional access system. He stated that DBS providers are prohibited by law from displaying local broadcast channels outside of their local areas, and therefore Mr. Roll's elements of the conditional access system may need another element for DBS that allows DBS providers to ensure that local channels are not shown outside of their local areas. Mr. Medin said that he believed that the committee could address this via inputs, meaning the information that identifies who the subscribers are and what they are allowed to access.

Mr. Hess said that MVPDs often do not have the contractual rights to pass through guide data; Mr. Medin said that is a business issue that their companies could address. Mr. Card said that not all contractual terms are business issues, and gave the examples of robustness and renewability. Ms. Neplokh agreed that the examples that Mr. Card raised are within the scope of the committee.

Inputs / APIs

Ms. Neplokh then sought comment on the information that a device would need to provide for a downloadable solution to work. She identified a content request, and an authentication message. Mr. Love suggested a man-machine interface that would provide the status of the security module for troubleshooting. Mr. Card said that the system will need to account for retail device authentication and subscriber authentication, and using them when consumers attach new equipment to the service; he called this process "provisioning management." He explained the importance of knowing exactly where a device and subscriber are located because accurate location information is necessary to follow local broadcast signal delivery laws. Mr. Messer encouraged the group to consider this in the context of mobile devices as well. Brant Candelore said that existing solutions like DLNA CVP-2, RVU, or HTML5 Remote User Interface may be the best way to address these issues.

Federal Advisory Committee Act (FACA) Overview

Paula Silberthau gave an overview of FACA, and explained that the committee needs to follow FACA to ensure that the agency can rely on the report that the committee submits. Ms. Silberthau explained that working groups can be non-public and gather information to present to the entire committee. She said that under FACA, the working groups need to be comprised of fewer than half of the committee members to ensure that there is not a quorum (individual members can be invited to make a presentation, if necessary for fact gathering purposes). She said that the working groups present their work to the full committee, which then votes on the working groups' recommendations. She said that the three guiding principles of FACA are openness in government, diversity and balance in perspectives, and public accountability.

Address by FCC Chairman Tom Wheeler

Chairman Wheeler thanked the committee members for donating their time to a complex task. He reiterated that the statute requires specific recommendations to achieve a downloadable software-based security solution, and said that the committee is up to the task.

Identification of Interested Parties and Their Ideal Experiences

After discussion, the committee identified five main groups of interested parties: (i) end users/subscribers, (ii) retail vendors/equipment manufacturers, (iii) MVPDs/content delivery companies, (iv) manufacturers of system equipment, and (iv) content owners/copyright holders.

End users

Dr. Ansari and Mr. Hess stated that the end user/subscriber experience should maintain the features and applications that are specific to their services. Mr. Medin said that as a retail CableCARD device user, he is able to customize his user interface and integrate over-the-top services, but is unable to receive on-demand services from his MVPD, and he would like to access those services. He said that simplicity is essential for consumers. He also said that not all consumers want the ability to access all of the services offered over an MVPD system. Mr. Goldberg said that the ideal consumer experience is to be able to buy a device, bring it home, plug it in, and have it work. He also said that it is important to consumers to have a range of devices to purchase from high-end devices with many features to low-end devices with few features.

Mr. Rolls said that a lot of the features that MVPDs offer are cloud-based, and are developed to run on legacy equipment. He said that it is easiest to offer those services via apps. Mr. Medin said that user experiences can coexist—the MVPD can offer one, but competing user interfaces will allow consumer electronics devices to differentiate themselves from one another—and that it is technically feasible to allow them to coexist.

Retail Device Manufacturers

Mr. Goldberg said that as long as the inputs and outputs of the security system are well defined, it should be easy for retail device manufacturers to build compatible devices. Mr. Medin said that device manufacturers may not want to rely on a single architecture: some may want to build downloadable security into every device, while others may want to build a single gateway device and network with screens throughout a home. Mr. Rolls said that each device will need to include a system on a chip/hardware root of trust. Mr. Messer said that there may be different solutions for different delivery methods (specifically, mobile devices may have a different solution than in-home set-top boxes). Mr. Hess and Mr. Clyne echoed this point, stating that a single standard might have precluded MVPD applications that run on mobile devices, and that Cablevision has over three million customers that use those applications.

Ms. Neplokh asked whether a device manufacturer could foresee what to build into a device to make that device compatible with MVPD services and applications. Mr. Hess said that it would not be possible to foresee prior to the development of Apple’s iOS and Google’s Android operating systems. Mr. Clyne said that it is a result of the industry moving in the application direction. Dr. Weber said that the benefit of a defined standard is that the device manufacturer does not need to wait for the MVPD to develop an application for its platform, and that standards allowed TiVo to develop a retail mobile solution before cable operators developed applications for mobile devices.

MVPDs

Mr. Card said that to his knowledge, DISH and mobile device manufacturers have had limited dialogue, and the reason that applications can run on those devices is because the device manufacturers understood the demands of content owners. Mr. Card said that established platforms help prevent MVPDs from having to communicate with each retail manufacturer. Mr. Murray asked whether a clearinghouse or certification process would help set rules of the road. Mr. Medin said that certification processes like DTLA and standards like HDCP are used in contracts with content companies today.

Mr. Card, Dr. Ansari, Mr. McClelland, and Mr. Murray discussed the boundaries of the security aspects, whether and how they are tied to the user experience, and how the committee should address those issues.

Mr. Rolls said that much of Charter's service development is happening in the cloud, outside of the set-top box.

System Equipment Manufacturers

Mr. Smith agreed that a lot of innovation is taking place in the cloud. He said that TV Everywhere builds elements including permissions, aspect ratio, and DRM into the application to work on each specific device, and that it is an affordable solution for small cable operators.

Content Companies

Mr. McCoskey said that agreements between content owners and MVPDs drive the technical specifications that are necessary to protect content. He said that many of the technical specifications exist today, and pointed to MovieLabs's specifications for protecting UltraHD, 4K content. He concluded that the market has satisfied content companies' needs.

Mr. Hess raised the issue of overlays and branding content with user interfaces, and asked for Mr. McCoskey's position on those. Mr. McCoskey said that those are covered by complex contracts between MVPDs and content companies. Mr. Goldberg stated that he believed that this was a policy issue rather than a technical issue.

Working Groups

Mr. Card proposed three working groups: (1) existing commercial standards, (2) technology and current architectures, and (3) future trends. The commercial requirements working group would gather information about the current business needs and legal requirements of the interested parties. The technology and current architectures working group would gather information about the different technologies that interested parties use. And the future technologies group would gather information about technologies that interested parties may rely upon in the future.

The group also requested that Ms. Neplokh summarize her guidance on the scope of the working group's mandate.

Future DSTAC Meeting Dates

Mr. Murray announced that future DSTAC meetings would take place on March 24th, May 13th, July 7th, and August 4th.

Comments from the Public

Alex Nevelson, an independent security consultant to the cable industry, stated that with respect to scope, replacing CableCARD would be an easy task, but developing a new ecosystem would be quite difficult.

On behalf of Veramatrix, Jim Williams of Media Strategies and Solutions stated that the DSTAC should look to the entire industry of downloadable security standardization and realize that diversity is an important part of security—otherwise you offer a single point of attack.

Steve Effros of Beyond Broadband Technology stated that the DSTAC should focus on technical issues like trusted authorities and threat targets rather than policy issues.

Mr. Murray adjourned the meeting at 3:02PM.

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Brendan Murray
Designated Federal Officer
Downloadable Security Technology Advisory Committee

Cheryl Tritt
Chairperson
Downloadable Security Technology Advisory Committee

These minutes will be formally considered by the Advisory Committee at its next meeting, and any corrections or notations will be incorporated in the minutes of that meeting.