Christopher Heimann
General Attorney &
Assistant General Counsel

AT&T Services, Inc.
1120 20th Street NW, Suite 1000
Washington, D.C. 20036
Phone 202 457-3058
Fax 202 457-3074

November 16, 2007

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, N.W.
Washington, D.C. 20554

Re: *Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronic Equipment,* CS Docket No. 97-80; PP Docket No. 00-67.

Dear Ms. Dortch:

As AT&T previously has demonstrated, and the record in this proceeding confirms, the two proposed standards for ensuring bidirectional compatibility of cable television systems and consumer electronics equipment currently being considered by the Commission (*i.e.*, OCAP and DCR+[1]) were designed specifically, and only, for digital cable systems employing QAM modulation, and thus are wholly inapplicable to the services and systems of MVPDs using different technologies or network architectures (including AT&T's IP-based U-verse service and DBS), which were not involved in development of those standards. Even the principal proponents of these standards (NCTA and CEA) concede as much, and therefore do not advocate that their proposed standards should apply to alternative MVPDs or even that their proposals offer a path toward an all-MVPD standard (assuming such a standard is feasible, which it currently is not).[2] As discussed further herein, imposing either proposal on alternative video delivery platforms – even if feasible – likely (and, in AT&T's case, certainly) would require competitive MVPDs to completely redesign their networks and systems, at enormous time and expense, as well as the risk of delaying (or even preventing) development and deployment of new and innovative features and services. It also could (and, in AT&T's case, would) jeopardize the security of alternative MVPDs' systems and content, and threaten further investment in and development of new technologies and services, contrary to Congress's express mandate that the

[1] DCR+ is not even a standard at this point insofar as specifications for DCR+ have not yet been fully developed, vetted and tested; nor have all necessary test suites, tools and the validation process for DCR+ been developed.

[2] NCTA Comments at 72-73 (acknowledging that its approach "will not provide consumers with a product that is fully portable to many MVPD providers available today"); CEA Comments at 13, 15 (acknowledging that enhancing navigation device availability for MVPD services other than digital cable systems is only a "potential[ity]" at this time, and conceding that, while such a solution "may be feasible," one has not yet been developed).

Commission encourage "development [and] introduction of . . . new and improved multichannel video programming or other service[s]."[3]

In what follows, AT&T first explains (by way of background) how IPTV services and systems, such as its U-verse TV service, fundamentally differ from digital cable systems employing QAM modulation, and specifically in how content is delivered and other critical functions (such as signal security and conditional access) are performed. Next, we explain why both of the proposed QAM-based standards at issue here (both of which are predicated on the CableCard specifications developed for the legacy cable industry with no input from competitive MVPDs) are fundamentally incompatible with, and could not be supported by AT&T's system – at least not without a complete overhaul of its network, at enormous time, expense, and the loss of system flexibility necessary to provide new and innovative features, functions and capabilities.

A. AT&T's IPTV Network and Operations Differ Fundamentally from Cable.

Historically, cable systems have been (and generally continue to be) designed to operate as one-way, passive distribution systems that retransmit broadcast television signals and linear cable channels to subscribers over coaxial cable. Cable operators generally take over-the-air TV signals, which are broadcast over 6 MHz of RF spectrum, and package them together with cable programming (delivered by satellite or, in some cases, terrestrially to cable system headends) for rebroadcast to subscribers over cable. Cable systems broadcast their entire content stream to all subscribers, assigning each over-the-air TV signal and cable channel to a separate band of RF spectrum. To watch a particular channel, a subscriber uses a tuner (in her TV or set-top box) to tune to the specific frequency over which the selected programming is transmitted.

Because cable networks broadcast their entire content stream to all subscribers, cable systems must rely on devices at the customer's premises to perform the conditional access functions of allowing individual subscribers selective access to and denial of specific services. These functions are performed by transmitting encryption keys, which interact with the conditional access systems residing on a subscriber's receiver or navigation device to descramble and permit access to specific programming and other content. Interaction between the network and a subscriber's CPE (beyond the one-way transmission of programming and other services from the network to the subscriber's CPE) is very limited, with the cable operator relying on the conditional access systems at the customer's premises to determine which services the subscriber may access. For two-way services (such as high speed Internet access and VOD), traditional cable systems designate a specific portion of the available spectrum for upstream communications (typically in the 5-40 MHz frequency band), and then broadcast the requested

---

[3] 47 U.S.C. § 549(c) (requiring the Commission to waive any regulation adopted pursuant to section 629 upon a showing that such waiver is necessary "to assist the development or introduction of a new and improved multichannel video programming or other service"). *See also Implementation of Section 304 of the Telecommunications Act of 1996*, Report and Order, 13 FCC Rcd 14775, paras. 16 and n.23, 132 (1998), *quoting* S. Rep. No. 104-230 at 181 (1996) (Conf. Rep.) (admonishing the Commission, in implementing section 629, to "avoid actions which could have the effect of freezing or chilling the development of new technologies and services").

content downstream over shared facilities to all subscribers (or to every node in the system), again relying on devices at the customer's premises (or the node) to prevent unauthorized viewers from accessing content.

AT&T's IPTV service is designed and operates in a fundamentally different manner. Unlike cable's broadcast architecture, AT&T's network employs an IP-based, interactive client-server architecture that requires constant communication between a subscriber's CPE and the network, and transmits to each subscriber only the specific programming the subscriber selects at a particular time, together with encryption keys necessary for the subscriber's media controller (*i.e.*, set-top box, or client-device) to decrypt that programming. That network is comprised of multiple server groups, including, *inter alia*: authentication servers, which determine whether a subscriber has rights to receive service; operational or business support system servers, which perform digital rights management functions to determine which particular programming and other services a subscriber is entitled to access and view; media acquisition servers, which acquire programming from a variety of content sources (including over-the-air and satellite-delivered programming); and media delivery servers, which distribute specific programming and other content when requested by a subscriber. All of these servers are linked together, and with client devices, by a common thread (or middleware) that resides both in the network and on client devices.

The following is a high-level overview of the way in which AT&T's network operates:

- First, AT&T acquires and processes content via network acquisition servers, which obtain live television services (including in-bound rights information associated with such content) from content providers, encrypt the content, generate encryption keys, and transmit the content, encryption keys and digital rights information (DRM) to one or more distribution servers, which, in turn, "distribute" such content upon request to subscribers.

- Second, whenever a subscriber turns on her television, her client (or navigation) device must "log-on" to the network (that is, be authenticated by and registered on the network) to obtain video programming. Once the client device has been authenticated, AT&T's video distribution servers transmit a session key that allows the client device to communicate with the servers and decrypt data (including channel keys necessary to decrypt specific programming) transmitted by the Video Servers, as well as a channel map identifying the video content available in a particular area (including channels to which the customer may not be subscribed).

- When a subscriber selects a particular channel from the program guide, her client device transmits a request to AT&T's video servers, which communicate with other servers and databases to determine whether the subscriber is authorized to view the channel selected

and, if so, deliver the requested content (together with the keys necessary to decrypt that content)[4] to the subscriber.

Thus, in AT&T's IP-based network, "conditional access" and other security functions are performed in the network (unlike traditional cable systems, which perform such functions in a set-top box), and require constant interaction and communication between a client device and the network to determine whether a particular end user is an authorized subscriber to AT&T's service and has rights to access and view the specific content requested by the subscriber.

B. Application of DCR+ or OCAP to U-verse Would Require AT&T to Completely Overhaul of Its Network.

Both OCAP and DCR+ are middleware platforms based upon the CableCard standard developed by CableLabs, and were designed specifically, and only, to operate on digital cable systems using RF/QAM modulation to deliver video content. Those platforms also are predicated on a conditional access security model (in which video signals and content are secured by securing the link between the network and subscriber through conditional access mechanisms in CPE – *i.e.*, the set-top box or CableCard), and use proprietary signaling and other protocols designed by the cable industry for use with traditional digital cable systems, and without input from competitive MVPDs using different technologies. The OCAP and DCR+ proposals thus are designed for an entirely different network, utilizing (*inter alia*) different technologies, security systems, and signaling protocols than AT&T's IPTV network and service. And application of those standards to AT&T would require it to completely redesign its network, at enormous expense, and sacrifice much of the flexibility offered by IP-based video technologies to offer new and innovative services

As discussed above, AT&T's IPTV service utilizes a highly-interactive, IP-based, client-server architecture that requires constant communication between client-device middleware residing in CPE and network middleware running on servers in the network. OCAP and DCR+ are client-device middleware application and signaling platforms designed to interact with and control cable's legacy broadcast distribution infrastructure. They are not designed to interoperate with the point-to-point client-server distribution architecture of IPTV. Insofar as OCAP and DCR+ have defined specifications only for client devices to access and control cable broadcast technology, specifications for client-server IP-based network middleware would have to be developed for implementation within the AT&T network, which likely would take considerable time and expense. It bears emphasis, in this regard, that all of the routers, servers and other equipment in AT&T's network that are used to acquire and distribute content, authenticate end-users, deliver interactive applications, and provide the electronic programming guide, VOD and DVR capability all depend on network middleware interacting with middleware on client devices. In short, requiring AT&T to comply with any OCAP or DCR+ based standard would require AT&T to completely overhaul its network and client software, in which AT&T already

---

[4] These keys are updated and sent to the client device (if that device is logged on to the system) at regular intervals. Consequently, the client device is in constant communication with the network, even if the subscriber has not changed channels and is unaware of such communication.

has invested hundreds of millions of dollars. The cost and time of so doing would simply be astronomical.

But the impact on AT&T of applying OCAP or DCR+ to U-verse is not limited only to the cost and time it would take to develop and deploy OCAP or DCR+ compatible network and client-device middleware. It also would have a profound impact on the services AT&T could offer, as well as the way in which it could offer those services. For example, as noted above, AT&T's network utilizes a client-server architecture in which the applications are based largely in the network, and require interaction between servers in the network and client devices, whereas applications in traditional cable networks run directly off the edge device (CPE) at the customer's premises. OCAP and DCR+ do not account for this difference, and assume a network in which applications are run directly off a client device rather than network-based applications. If either proposal were mandated for all MVPDs by the Commission, AT&T could be forced to alter the applications environment on its system, again at significant cost and lost efficiency (insofar as any change in applications would require implementation in every client device connected to the network rather than simply changing the application in the network itself).

Additionally, OCAP and DCR+ use application programming interfaces (APIs) and signaling protocols (which are used to communicate with the network to deliver on-demand services, like VOD) that are based on proprietary protocols designed by CableLabs and the cable industry. Because of their origin, these technologies have no allowance for the development of realtime client-server applications that are predominant in an IPTV network architecture.

In contrast, AT&T's application platform is based upon open IP-based standards common in the Internet and information technology sectors today, which provides AT&T significantly greater flexibility in software and application design on its distributed architecture. This flexibility is critical to AT&T's success in the market insofar as that success depends to a significant extent on AT&T's ability to differentiate itself and offer innovative features, functions and capabilities to its customers. Because OCAP and DCR+ middleware limit the type of applications that can be implemented to those based on legacy cable services (for which OCAP and DCR+ were designed), requiring AT&T and other competitive MVPDs to implement those proposals would prevent those competitors from offering a differentiated consumer experience made possible through their innovative architecture, hampering their ability to compete. In the end, consumers will be the losers, as they are deprived of the benefits of robust competition, including innovation and investment in new services.

Finally, adoption of an all-MVPD standard based on OCAP or DCR+ would require AT&T to completely alter the way in which it secures its network and protects content delivered to subscribers. OCAP and DCR+ are based on a conditional access model in which the content stream – rather than specific content within that stream – is protected. In this model, the link between the network and the subscriber is secured, and, once that link is open, the content traveling on the pipe is available without additional security or protection. In contrast, as discussed above, security in an IPTV system, like AT&T's, is based on digital rights management (DRM) in which not only the content stream but also specific content within that stream is protected through separate encryption of both the content (program-by-program) and

the signal (as discussed above, a subscriber that logs on to the network is provided both a session key to decrypt the signal and a channel key to decrypt specific content). In this model, digital rights information for content is stored on the network, and is transmitted – together with that content and channel keys necessary to decrypt such content – only to subscribers that are authorized to view or otherwise access that content. In short, neither OCAP nor DCR+ is designed to accommodate DRM, which is inherent in IPTV generally, and AT&T's network in particular. Adoption of either proposal as an all-MVPD standard thus would require modification of those standards to accommodate DRM (which could not be done over night), or force competitive MVPDs, like AT&T, relying on DRM to abandon DRM in favor of traditional conditional access security – which inherently are less secure than DRM, which would run afoul of Congress's proscription against adoption of any regulation that would jeopardize security of programming and other services.[5]

For these reasons, and those set forth in AT&T's previous filings in this proceeding, the Commission should not impose DCR+ or OCAP on non-QAM based video service providers using different technologies or network architectures. If you have any questions concerning the foregoing, please do not hesitate to contact me at 202-457-3058.

Sincerely,

/s/ Christopher M. Heimann

cc: Michelle Carey
Monica Desai
Rick Chessen
Rudy Brioche
Amy Blakenship
Christina Pauze
Mary Beth Murphy
Brendan Murray
Michael Lance
Steven Broeckaert

[5] 47 U.S.C. § 549(b).