**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Implementation of Section 304 of the Telecommunications Act of 1996 | ) | CS Docket No. 97-80 |
| | ) | |
| | ) | |
| Commercial Availability of Navigation Devices | ) | |
| | ) | |
| | ) | |
| Cable Industry Report on Downloadable Security | ) | DA 05-3237 |
| | ) | |

# COMMENTS OF DELL INC., HEWLETT-PACKARD COMPANY, INTEL CORPORATION, AND SONY ELECTRONICS INC.


**DELL INC.**

Neeraj Srivastava
Director, Client Architecture & Technology
Dell Inc.
One Dell Way
Round Rock, Texas 78682-8033

**HEWLETT-PACKARD COMPANY**

Adam Petruszka
Director, Strategic Initiatives
Office of Strategy & Technology
Hewlett-Packard Company
2055 State Highway 249
MS-110225
Houston, TX 77070

**INTEL CORPORATION**

Jeffrey T. Lawrence
Director, Content Policy and Architecture
Intel Corporation
JF3-147
2111 N.E. 25th Avenue
Hillsboro, OR 97124-5961

**SONY ELECTRONICS INC.**

Jim Morgan
Director & Counsel
Government & Industry Affairs
Sony Electronics Inc.
1667 K Street, NW
Suite 200
Washington, DC 20006


January 20, 2006

**TABLE OF CONTENTS**

**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Implementation of Section 304 of the Telecommunications Act of 1996 | ) | CS Docket No. 97-80 |
| | ) | |
| Commercial Availability of Navigation Devices | ) | |
| | ) | |
| Cable Industry Report on Downloadable Security | ) | DA 05-3237 |

**COMMENTS OF DELL INC., HEWLETT-PACKARD, INTEL CORPORATION, AND SONY ELECTRONICS INC.**

Dell Inc. ("Dell"),[1] Hewlett-Packard Company ("HP"),[2] Intel Corporation ("Intel"),[3] and Sony Electronics Inc. ("Sony")[4] (collectively, the "Companies") hereby submit these comments in response to the Report of the National Cable & Telecommunications Association on Downloadable Security ("NCTA Report") and the accompanying Downloadable Conditional

---

[1] Dell Inc. is a trusted and diversified information-technology supplier and partner, and sells a comprehensive portfolio of products and services directly to customers worldwide. Dell, recognized by Fortune magazine as America's most admired company and No. 3 globally, designs, builds and delivers innovative, tailored systems that provide customers with exceptional value. Company revenue for the last four quarters was $54.2 billion. For more information about Dell and its products and services, visit www.dell.com.

[2] HP is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, global services, business and home computing, and imaging and printing. For the four fiscal quarters ended Oct. 31, 2005, HP revenue totaled $86.7 billion. More information about HP is available at http://www.hp.com.

[3] Intel, the world leader in silicon innovation, develops technologies, products and initiatives to continually advance how people work and live. Additional information about Intel is available at www.intel.com/pressroom.

[4] The U.S.-based electronics unit of Sony Corporation of America and the Sony Corporation, Sony Electronics Inc. manufactures and sells personal computers through its VAIO division.

Access System Host License Agreement (the "DCAS Agreement")[5] submitted by the National Cable & Telecommunications Association ("NCTA") in the above-captioned proceeding.[6]

## INTRODUCTION AND SUMMARY

Although the Companies generally support the move to truly downloadable security, we are not able to support the downloadable security regime outlined in the NCTA Report because that regime will not result in a truly competitive market for cable-compatible navigation devices. Instead, it will effectively preclude the makers of multi-function devices like personal computers from participation in that market. Because the NCTA Report does not provide a reasonable alternative to the current requirement that cable operators cease providing integrated set-top boxes by July 1, 2007, the Commission should inform the cable industry that it must comply with that deadline.

At the same time, the Companies continue to support the development of a truly downloadable content security mechanism. In the interests of developing such a regime, the Commission should inform the cable industry that it will entertain a further submission that revises the downloadable security model to ensure that all consumer product manufacturers have reasonable access to that market-segment. The Commission also should urge the cable industry to discuss future downloadable access specifications with interested parties from the consumer electronics and personal computer industries, so as to facilitate a truly competitive market-segment for cable-compatible navigation devices.

---

[5] The downloadable conditional access system described in the DCAS Agreement is referred to herein as the "DCAS."

[6] *See* Media Bureau Announces Dates for Filing Comments and Reply Comments on Cable Industry Report on Downloadable Security, *Public Notice*, DA 05-3237 (released December 20, 2005); Implementation of Section 304 of the Telecommunications Act of 1996, *Order*, CS Docket No. 97-80, DA 05-3316 (released December 23, 2005).

Because the trend toward integrating various digital content processing devices (including set top boxes, digital televisions, media players, ad computing devices) is likely to continue, it is essential that the Commission do all it can to ensure that the downloadable security model that the cable industry adopts will be flexible enough to evolve as equipment evolves. If it does not, then the Commission will be forced to review agreements like this serially, because a new content protection regime will be needed each time technology overleaps the protections that the cable industry puts into place.

## BACKGROUND

The NCTA Report and the DCAS Agreement represent the cable industry's (and, presumably, content providers') proposed next step in the development of so-called "Plug and Play" television receivers that are expected to eliminate the need for cable set top boxes by incorporating signal decoding and content security functionality in the television receivers themselves. As traditional television receivers have moved towards Plug-and-Play, concurrent technological developments and consumer demands have led to the convergence of traditional stand-alone television sets and alternative multi-function devices like personal computers. Today, the word "television" just as easily could refer to a personal computer with a television tuner card as to a traditional stand-alone television receiver. As our customers increasingly demand greater video functionality from their personal computers and the ability to link multiple home entertainment devices into home networks, our interest in ensuring them a seamless viewing experience grows. Consequently, the development of Plug-and-Play technology now concerns computer manufacturers like the Companies just as much as it does the consumer electronics industry.

As one of the leading manufacturers of microprocessors and converged computing and communications equipment, Intel has for the past several years taken an actively participated in

the Cable Plug-and-Play proceedings both before the Commission and in the bi-directional negotiations. In the Plug-and-Play context, Intel always has taken the view that the evolution of television receivers from single-function pieces of furniture to multi-function components of a larger home-network of interrelated devices requires a rethinking of the approach taken by industry and regulators to technical standards and device interoperability.

Throughout its participation in FCC proceedings and private industry negotiations regarding Plug-and-Play devices, Intel has advocated four key principles that should guide government and industry in Plug-and-Play. These principles, which all of the Companies fully endorse and reiterate today, include:

1. **Consumer Choice.** The specifications and license requirements for cable-compatible Plug-and-Play devices should be flexible enough to allow for the incorporation of Plug-and-Play capability in a wide range of consumer electronics and information technology devices, including traditional stand-alone televisions, cable and satellite set-top-boxes, digital video recorders, game consoles, personal computers, and other multi-function devices. Neither the specifications themselves nor the robustness, compliance, and certification rules that govern licensing of necessary technology should preclude any particular class or type of machine from participating in the market for Plug-and-Play devices. Indeed, a truly competitive retail market depends on device manufacturers' freedom to innovate and consumers' freedom of choice. Just as the Commission should not attempt by regulation to pick technology "winners" and "losers" (but rather let consumers decide which technologies best meet their needs), the Plug-and-Play process and agreements related to it should not have the effect of ensuring that certain types of products – such as cable-card enabled stand-alone televisions – will be capable of delivering on

evolving consumer expectations while others –such as personal computers--are sidelined. Consumers should make those choices.

2. **Consumer Control.** As technological advances provide consumers with new, multi-functional products and innovative ways to link those devices, consumers should have the right to control their own machines and configure and control their own home-networks in the manner that best suits their individual needs. In the Plug-and-Play context, this means that whatever conditional access technologies are adopted by industry must be versatile enough to preserve consumers' right to move lawfully acquired content from one device in the home network to another without complicating the viewing experience. Realistically, preserving consumer control will require a conditional access technology licensing scheme that designates a reasonable number of approved protected output technologies with sufficient diversity to ensure that the many potentially interoperable home video devices can be seamlessly woven into home networks.[7]

3. **Common Reliance.** Creating a competitive market for television navigation devices that actually will serve consumers' needs and desires requires "common reliance" standards for security technology and conditional access interfaces. Content providers, device manufacturers, and the cable industry must work from the same set of security standards to create a market where manufacturers compete on the basis of product quality and price rather than on their access to proprietary security information. From a consumer perspective, common

---

[7] A number of specifications for secure outputs that perform these tasks already have been developed and adopted by various industry groups, including the Digital Transmission Content Protection ("DTCP", which has been mapped to several interfaces, including, *e.g.*, Internet Protocol ("DTCP IP") and IEEE 1394 ("DTCP 1394"), High-Bandwidth Digital Content Protection ("HDCP"), and Windows Media Digital Rights Management ("Windows Media DRM").

reliance means that consumers can count on their products working as advertised for a reasonable period of time, without having to worry that changes in content protection technology will render devices obsolete. Common reliance also ensures that manufacturers can be confident that their devices will be compatible from a security standpoint with other devices utilizing the same standards. As the Commission has recognized, the use of common reliance standards plays a key role in fostering a competitive market in navigation devices because it places all manufacturers and devices on a level playing field with those produced by the cable industry with respect to their security capabilities.[8] The Companies agree with this assessment and encourage the Commission to continue insisting that common reliance standards be a part of any Commission-approved security or output regulations for Plug-and Play.

4. **Software-Based Downloadable Conditional Access.** The Companies have advocated, and continue to support, the move to a software-based downloadable conditional access system based on common reliance standards. This is the best way to provide consumers with the choice and control described above, without compromising cable operators' legitimate interest in network integrity or content providers' reasonable concerns about illegal copying. To accomplish these goals, however, a downloadable conditional access system should consist chiefly of a software application that can be downloaded onto a general purpose computing platform. Such a system should make a minimum of demands on the hardware that composes the computing platform itself and specify proven and economically viable security features that can be implemented across multiple general purpose platforms or to dedicated products. Examples of such systems are the Windows Media DRM and the Open Mobile Alliance DRM

[8] Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices, *Second Report and Order*, 20 FCC Rcd 6794, ¶ 27 (2005).

2.0, which are software-based platforms that can be updated to defeat the efforts of successful hackers. True downloadable access control will rely on few, if any, hardware requirements, taking advantage of software renewability. If hardware requirements are associated with a general purpose conditional access platform, such requirements should be based on manufacturer implementation of an open standards-based hardware security feature, not on proprietary technology. This will assure that device manufacturers will not be excluded from the market by a requirement for proprietary hardware that is incompatible with their underlying platform.

These four key principles – consumer choice, consumer control, common reliance, and software-based downloadable conditional access – should guide government and industry in the Plug-and-Play debate. However, as discussed below, the NCTA Report and accompanying DCAS Agreement are inconsistent with these principles in a number of ways that ultimately will harm consumers and device manufacturers. Most troubling to the Companies, the DCAS Agreement appears to preclude the incorporation of downloadable security in most multi-function devices and in all personal computers as those devices currently are constructed. Because potential licensees cannot even access or review the specifications for the licensed technology, determining for certain the extent to which the technology can be implemented on the personal computer platform is impossible.[9] At the same time, however, several features of

---

[9] DCAS Agreement § 2. Indeed, to view the DCAS specifications, a potential licensee must sign not only the DCAS Agreement, but also the Digital Certificate Authorization Agreement, the CableCard Host Interface License Agreement and the Open Cable Applications Platform License. *Id.* § 2.8. Once a potential licensee has signed these agreements, the company still must face security review by NGNA, LLC, which may apply additional standards regarding handling of security keys. *Id.* The level of secrecy surrounding the DCAS standards and the prior commitments that CableLabs requires before allowing licensees to view the technical specifications appears inconsistent with the Commission's rules requiring multichannel video providers to make available technical data necessary to enable navigation devices to function in conjunction with cable systems. 47 C.F.R. § 76.1205.

the License Agreement itself indicate incompatibility between the DCAS regime and personal computer architecture. Indeed, we anticipate that compliance with the DCAS Agreement would necessitate changes in architecture and design that would change the very nature of the personal computer.

## I. DCAS IS NOT A TRUE DOWNLOADABLE CONDITIONAL ACCESS REGIME.

The most basic issue with the conditional access model outlined in the NCTA Report and the DCAS Agreement is that it does *not really* offer downloadable conditional access. Instead, DCAS appears simply to have replaced one proprietary hardware requirement (the CableCard) with another (a secure microprocessor, etc.).[10] For stand-alone DTV receivers and traditional set-top boxes, this may be an acceptable solution. But for multi-function devices like personal computers, the requirement of a proprietary, secure microprocessor and enhanced video memory robustness requirements makes integration of the video receiver into the device's other functionalities extremely difficult and expensive, if not impossible.[11]

Downloadable security systems should rely on renewable software rather than proprietary hardware regimes. If, however, a hardware requirement must be implemented along with DCAS, it should be based on an open-standards approach, specifying the technology that allows individual manufacturers the flexibility to develop their own compliant hardware. This approach has a number of advantages, which were recognized by the cable industry when it used an open-standards approach to implementation of the Data Over Cable Service Interface Specification ("DOCSIS") standard in cable modems. For example, it allows device manufacturers to develop

---

[10] NCTA Report at 3. "Secure Microprocessor" does not seem to be defined anywhere in the NCTA Report, the DCAS Agreement, or the accompanying Robustness Rules and Compliance Rules.

[11] DCAS Agreement, Exhibit B §§ 1.4, 3.

hardware that complies with general standards, can be used for multiple purposes on the device, and is compatible with other hardware contained in the device. Because it requires the least amount of system redesign, the open-standards approach also permits manufacturers to minimize costs, facilitating market entry. Moreover, the open-standards approach ensures that NCTA and CableLabs will not have an effective veto power over the internal architecture of consumer electronics devices. This is a particular concern for manufacturers of multi-function devices like personal computers, into which video reception capability is but one of many functions to be integrated. An open standards model also ensures that the owner of the proprietary security hardware will not gain a competitive advantage in the market by establishing license terms and conditions that have the effect of excluding certain market participants.

Unfortunately, the NCTA Report and the DCAS Agreement do not satisfy these principles. What NCTA has offered is not really a software-based solution, but rather a hardware-based solution with what appears to be a small downloadable software component. Although the Companies recognize the benefits to the consumer of eliminating the cable card requirement, and understand that the configuration presented by the NCTA Report ultimately *may* offer cost savings to some, NCTA's solution: (1) does not represent truly software based downloadable security; (2) is not based on open standards; and (3) can, from what we can glean from the Report, be implemented on few, if any, truly multi-function devices like personal computers.

For these reasons, encouraging DCAS, as described in the NCTA Report and DCAS Agreement, to become the standard for cable compatible navigation devices would not further

the Commission's statutory directive to ensure a competitive market for those products.[12] Nor would it lead to the type of innovation and dynamic development that has characterized multi-function devices like personal computers throughout their history. Instead, DCAS would entrench the current stand-alone model for television navigation devices represented by televisions and set-top boxes. The failure to ensure a competitive market for navigation devices ultimately will trickle down to consumers in the form of fewer choices and higher prices.

## II. DCAS WOULD UNDULY CONSTRAIN CUSTOMER CHOICE.

In addition to likely precluding a truly competitive market for navigation devices, the DCAS regime proposed by NCTA will constrain consumer choice by limiting the types of products that may utilize the DCAS Agreement. The DCAS implementation limitations suggest that the types of devices that will be able to incorporate DCAS and the functionalities those devices will be able to perform will be severely limited.

Despite the fact that the cable industry is moving towards two-way interactive services and the Internet already provides viewers with such functionality, the DCAS Agreement perpetuates a dated security model that is more appropriate for the quickly fading one-way video universe. The DCAS compliance and robustness rules require an unnaturally high level of security against tampering.[13] The arguments for these requirements, however, seem most suited to the one-way environment where there is no possibility for active authentication of users and

---

[12] 47 U.S.C. § 549.

[13] The DCAS Agreement and Robustness Rules also are unusual in that they appear to require that the licensee's system absolutely protects content rather than requiring a defined level of robustness (*e.g.*, the familiar "effectively frustrates" would-be pirates standard). *See* DCAS Agreement, Robustness Rules §§ 1.1, 1.4. For obvious reasons, it is all but impossible for a licensee to guarantee that its security systems will actually defeat would-be pirates in all cases.

no cost-effective means of pro-active renewal.[14] For example, the security requirements for the secure microprocessor are unnecessarily high.[15] Microprocessor security at the prescribed levels makes it harder to provide software updates, and the additional security is unnecessary because these devices will permit dynamic authentication of hardware. If the hardware has been tampered, it can be disabled remotely. Thus the additional hardware security amounts to overkill.

This pattern of overly-restrictive compliance and robustness rules is repeated throughout the DCAS Agreement. As another example, the Robustness Rules define the PCI Express component interface as a "user accessible bus" despite the fact that it is related to the PCI bus in name only. PCI Express clearly is an internal system point-to-point interconnect that does not transmit the same data on all of its connectors. As with many critical applications, transactions on the PCI Express are sufficiently protected at higher layers in software, in the same manner that banking transactions, for example, are protected. Only a well-funded pirate with a large and sophisticated engineering team (including manufacturing capabilities) could ever actually succeed in extracting usable content from PCI Express.[16] There is no reasonable purpose for this extra degree of security. Setting unnecessarily high security standards leads to unnecessary device costs – and thus higher prices for consumers – and potentially prohibits some manufacturers from entering the marketplace. Moreover, in the case of defining the PCI Express

---

[14] For example, in the broadcast flag context, broadcasters send out their content and customers are authenticated based upon a token they receiver via another path. With two-way services, however, duplication of a security token is immediately detectable and actionable.

[15] The Robustness Rules require the secure microprocessor to satisfy Common Criteria EAL 5+. Robustness Rules § 1.1.

[16] Robustness Rules § 3. The PCI Express issue is detailed more fully in comments filed today by ATI Technolgies, Inc., Dell Inc., Hewlett-Packard Company, and Intel Corporation.

as a "user accessible bus," the cable industry is, in effect, seeking to control the architecture of connected devices.

These issues are exacerbated by the fact that the DCAS License Agreement does not clearly articulate what a "Licensed Product" or "Host Device" is. Rather, those terms are defined generally to include essentially any bi-directional device that uses the DCAS technology. In this context, it is unclear whether a "dongle" that might plug into a personal computer is even an acceptable implementation, or whether CableLabs would deem the entire personal computer to be part of such a "dongle" implementation. In light of CableLabs' historical reliance on requiring specific "profiles" for almost every implementation, the Companies are concerned that CableLabs' intends to sweep the entire personal computer into the definition (for both a 'dongle' approach and a fully integrated implementation). Such a construction would subject the entire personal computer to all of the DCAS regime's robustness requirements, even though in fact, in a dongle implementation approach, the personal computer may be more accurately described as a sink device from an approved output than as a "host device." The effect of such an interpretation would be to subject personal computers to an unnecessary security standard that they could not practically meet.[17] Due to these limitations, the DCAS system appears to be an example of CableLabs implicitly excluding multi-function devices like personal computers from full participation in the Cable Plug-and-Play system.

---

[17] Moreover, the Robustness Rules indicate that CableLabs intends to continue to exercise tight control over the type and level of security offered by the DCAS system. Section 5 of the Robustness Rules, entitled "Update Procedure," requires a product to be capable of incorporating "new countermeasures" to defeat theft. This indicates that CableLabs intends to continue to dictate the manner in which licensed products must protect against security threats rather than just providing the rules and allowing for other entities to innovate and create new protection technologies that satisfy those rules.

This implicit exclusion of personal computer manufacturers follows a pattern laid down by CableLabs in the CableCard Host Interface License Agreement and the POD-Host Interface License Agreement. As with those licenses, the DCAS Agreement does not expressly exclude personal computers or other multi-function devices; instead it sets out unnecessary robustness and certification requirements that appear to be specifically intended to preserve the traditional set-top box as the dominant cable navigation device, or, at least to limit implementation to less complex additional devices like digital televisions.[18]

Thus, while NCTA presents its DCAS scheme as a generally available license that will permit consumer electronic manufacturers of all stripes to provide unidirectional cable products,[19] the reality appears to be that the only opportunity for personal computer entry into the navigation device market, if any, will be through tightly controlled, yet-to-be-negotiated, private agreements that may result in individual companies gaining the right to provide devices. An example of such an agreement is the one that produced the recently-unveiled Open Cable Unidirectional Receiver ("OCUR") designed to work with Microsoft's Window's Vista operating system. The Companies support Microsoft's ability to offer a unidirectional receiver and the right of all companies to negotiate agreements they believe are in their best interests. From a policy perspective, however, the DFAST License and its associated rules were approved by the Commission specifically for that purpose. Indeed, the very reason most computer companies supported the CEA-NCTA MOU and the associated DFAST License Agreement was

---

[18] Another example of the implicit exclusion of multi-function devices like personal computers is the requirement that video decryption engines and video decoders must be either within the "same silicon device or ASIC" or linked by encrypted interconnects. DCAS Agreement, Robustness Rules § 3. This requirement effectively precludes a software-based implementation of DCAS, requiring instead, the use of the proprietary hardware described in the NCTA Report.

[19] NCTA Report at 2.

the express statement and assumption by the parties that personal computer implementations were authorized under that regime.[20]

Although that was CableLabs' statement on the record, reality has not borne it out. First, CableLabs required a specific profile for the OCUR device that is not part of the DFAST regime; and second, the OCUR is not available to other implementers under the DFAST license. The license agreement offered in conjunction with OCUR differs in many material respects from the DFAST License.[21] The Commission should judge NCTA's statements regarding the flexibility of the DCAS potentially to include a diverse range of devices with the cable industry's history under the DFAST regime in mind. Indeed, the Commission could take a positive step for both consumers and device manufacturers by indicating that it would consider it an act of good faith for CableLabs to make the OCUR available under the DFAST License consistent with the spirit and intent of the unidirectional proceedings and associated agreements.

Even the OCUR, however, may fall short of satisfying consumer expectations for weaving their entertainment and other devices into a seamless home network. The OCUR will provide decoding and DVR functionality, but, in its initial form, at least, it will interface with only a single PC and will only be accessible by a limited number of devices in the home network. While such arrangements may give consumers a few limited options for using unidirectional cable products with their personal computers, this is far from the kind of consumer choice that would be offered by a highly competitive market open to all potential providers with

---

[20] Implementation of Section 304 of the Telecommunications Act of 1996, *Second Report and Order and Second Further Notice of Proposed Rulemaking*, 18 FCC Rcd 20893 n.32 (2003).

[21] Examples include the treatment of copy freely content (which requires protection under the OCUR Agreement), and outputs that are approved with the OCUR regime. Although, for example, DTCP is an approved output under DFAST, it is not an approved output from an OCUR device, which permits use only of the Windows Media DRM.

a variety of approved outputs. This is not the environment that the Commission should be encouraging. And approving DCAS will only perpetuate this environment.

## III. DCAS WOULD NOT PERMIT CONSUMERS TO USE THEIR HOME NETWORKS FOR CABLE-SUPPLIED VIDEO CONTENT.

One of the real promises of converged communications devices like the cable compatible personal computer is the possibility of linking multiple devices throughout the home, allowing consumers to seamlessly distribute programming from one device to another in a protected home environment with nothing more than a mouse click. It appears, however, that the DCAS scheme is designed to make sure that this promise is never kept; indeed, if personal computer designers and manufacturers cannot gain general access to the technology necessary to provide cable compatibility, then a source of news, public affairs, and entertainment – if not *the* major news, information, and entertainment source for most households– will remain outside the reach of the home network.

The cable industry's proposal of a DCAS regime that effectively excludes fully functioning home networks is consistent with their conduct over the past several years. Indeed, despite numerous attempts by the computer industry to engage in discussions with the cable industry, the DCAS Agreement does not address any of the computer industry's concerns regarding the need for license terms that: (i) facilitate, rather than hamper, the home network; or (ii) provide reasonable assurance of timely consideration and approval even of compliant output technologies that would make such networks possible.[22] In the context of open home networking,

---

[22] The DCAS Agreement's hostility to the development of home networks is demonstrated by several provisions that suggest Open Cable Access Platform license rules will apply to all downstream component of a home network. *See*, *e.g.*, DCAS Agreement, Compliance Rules, § 3.4.1. Requiring all downstream devices to be OCAP complaint would essentially give CableLabs control over the architecture of every device in the entire home network, a result incompatible with the consumer choice the Commission should be encouraging.

the Companies find NCTA's comparison of the DCAS Agreement to the Digital Transmission Content Protection ("DTCP") license agreement unpersuasive at best.

The NCTA Report inappropriately likens the DCAS licensing framework to the DTCP licensing scheme that governs licensing of a link-layer content protection technology that protects compressed content in the home network over various interfaces (including wired and wireless Internet Protocol, FireWire IEEE-1394, USB and other interfaces). A comparison of the two frameworks, however, shows the similarities are superficial at best, while the dissimilarities between the two highlight many of the deficiencies in the DCAS plan.[23] Indeed, the two licensing systems could hardly be more dissimilar.

For example, the DCAS Agreement asks computer manufacturers to surrender the right to assert patent claims on (what we may assume must be) a very complex secure microprocessor technology, without even being able to see the specification and therefore what rights they will be required to forego.[24] Although both DTCP (which concerns only a simple link protection scheme based on encryption and authentication) and DCAS both are based on a "non-assert" licensing structure, manufacturers can review fully the DTCP technical specification *before* committing to the non-asserts, whereas under DCAS, manufacturers must commit to surrender their right to assert intellectual property rights before they even know what is covered by the specification.[25]

---

[23] NCTA Report at 6-7.

[24] DCAS Agreement, § 2. Although the DCAS Agreement claims that the "family of specifications" DCAS licensees must accept are posted at www.opencable.com, no DCAS specifications are posted on that site. Indeed, Intel does not believe those specifications are available anywhere.

[25] Nor is this the only example of the DCAS Agreement showing a lack of respect for potential licensees' intellectual property rights. Under Section 2.1 of the Compliance Rules, all licensees

This blind non-assert condition is a decisive difference between the DTCP and DCAS licenses, and it is decisively unfair to device manufacturers. This is because while DTCP is a narrow technical specification defining encryption and authentication protocols and localization requirements, DCAS references technical specifications in the intellectual property-rich "trusted computing" arena. Information technology companies like Dell, HP, Intel, and Sony hold substantial intellectual property in that arena, but implementers are asked to commit all of that IP before they even have had a chance to review the DCAS specification.

DCAS also differs from DTCP with respect to the limitations it places on the technology implementation and the devices that can be produced consistent with the license. The DCAS Agreement appears to define and require very specific hardware, and it unnecessarily imposes robustness requirements that have the effect of precluding certain types of products and product architectures without regard for basic security requirements. In addition, the Companies fully anticipate that individual DCAS implementations will be the subject of detailed technical "profiles," and that certification will remain a challenging white water rafting expedition through an assortment of CableLabs certification waives and broad CableLabs discretion when granting or withholding certification.[26] The DTCP technical specification, on the other hand, is narrow, specifically targeting authentication protocols and the like. The DTCP license and specification

---

are required to execute a "robustness checklist" that requires licensees to reveal trade secrets and myriad implementation details. Although the rules permit licensees to seek a non-disclosure agreement, this is only a partial remedy for requiring disclosure of highly confidential information. These requirements are a marked departure from agreements such as DTCP.

[26] Moreover, even when certification has been attained, the DCAS Agreement retains for CableLabs the right to exercise change-management rules that can best be described as arbitrary. DCAS Agreement § 3. Although the change management process provides for input from all interested parties, final decisions are reserved to CableLabs, *see id.* (chart labeled "OpenCable Engineering Change Process"), and the DCAS Agreement contains only the barest explanations of what standards CableLabs will apply.

are implementation-agnostic. DTCP can be implemented in software, hardware, or combinations of both to promote innovation. This enables DTCP to be deployed in a wide range of devices. The DTCP license establishes generic security requirements and lets implementers decide how to meet those requirements, allowing implementers to self-certify their devices to remove artificial barriers to market entry, enhancing competition and benefiting consumers. In contrast, under the DCAS Agreement, all implementation is strictly controlled.[27]

Perhaps most important of all from a consumer standpoint, the DTCP licensing process has actually functioned to approve new outputs through a smooth-functioning and timely review process that proceeds according to well-defined standards. This facilitates the timely roll-out of new consumer devices that utilize DTCP technology. The DCAS Agreement does not define an approved output process for the DCAS Technology. And, although Cable Labs purports to have an approved output certification process for unidirectional DFAST devices, that process appears to be broken.[28]

In April, 2005, the Digital Transmission Licensing Administrator ("DTLA")[29] asked CableLabs to approve DTCP over Internet Protocol ("DTCP IP") as an approved output for unidirectional and bidirectional cable devices. Intel has worked actively with CableLabs to gain approval of DTCP IP as an output technology for unidirectional and interactive devices since that time. The ongoing certification negotiation for this new DTCP IP specification approval

---

[27] Indeed, implementation is so closely defined in the Compliance rules that licensees apparently would be precluded from developing more robust systems than that specified in the DCAS Agreement.

[28] The DCAS Agreement, § 1.4, indicates that documents outlining CableLabs certification procedures, particularly the "acceptance test procedure" and "DCAS Protocol Implementation Compliance Statements," are posted on the Internet at www.opencable.com/dcas. These document, however, are not posted at this website, or, so far as Intel is aware, anywhere else.

[29] DTLA founding members include Hitachi, Intel, MEI, Sony and Toshiba.

illustrates the difficulties with obtaining CableLabs' approval for any output technology, including even the most minor modifications of existing approved technologies. For example: (i) DTCP already has been broadly approved by CableLabs for both unidirectional and bidirectional devices over the 1394 interface; (ii) DTCP is, in fact, all but a regulatory requirement for digital set top box outputs; (iii) DTCP is "DTCP" regardless of the interface it protects; (iv) DTCP over the IP interface differs from DTCP over the 1394 interface only in that it has specific localization requirements added at the request of content providers; and (v) DTCP IP has gained the approval of a wide range of content industry and government standards-setting organizations. Nonetheless, DTCP IP still has not been approved by CableLabs in any license agreement for any type of content. By way of example, DTCP IP has been approved as an output technology:

- unanimously by the MPAA studio companies at the DVD Copy Control Association;
- for digital video content in Japan through the ARIB process; and
- by the FCC in the Broadcast Flag Proceeding.

DTCP IP also is currently included in the mandatory requirements of the Digital Living Network Alliance ("DLNA") guidelines that are working their way through the DLNA process.[30] Despite these approvals, CableLabs has yet to approve DTCP IP notwithstanding Intel's more than eight months of active engagement with them, due to what often appear to be shifting requirements.

Of course, without DTCP IP approval by CableLabs, no consumer devices that would utilize that technology can be produced. The delayed approval of DTCP IP illustrates the general problem with the DCAS and other Cable-Host Interface License Agreement ("CHILA") regimes. These agreements give CableLabs absolute discretion in approving new technologies, giving

---

[30] CableLabs itself is part of the DLNA's content protection committee.

them an inordinate power over what products reach the market – thus allowing CableLabs to pick technology "winners" and "losers." CableLabs' "slow roll" on DTCP IP appears to have nothing to do with security concerns (as evidenced by the already approved DTCP 1394) and everything to do with the cable industry's apparent strategy of maintaining strict control over the number and type of available output technologies. Indeed, given the content of the DCAS Agreement, CableLabs appears to have a strong preference for requiring that its own proprietary technology be included in as many digital outputs as possible.[31]

Consumers should not be deprived of innovative new technologies simply because the cable industry wishes to control the development of home networking. Yet, Commission acceptance of the DCAS Agreement as satisfying the security/decoding separation requirement would effect that result, because no multi-function platform will be able to satisfy the Agreement's provisions. Section 629 of the Act was designed to enhance, not erode, consumer choice and control over the video devices that consumers bring into their home and connect to their home network. The DCAS regime that NCTA has proposed would severely erode consumer choice and control without any meaningful enhancement in security.

## IV. NCTA'S DCAS PROPOSAL MUST UNDERGO SUBSTANTIAL CHANGES BEFORE THE COMPANIES COULD SUPPORT IT.

As the foregoing demonstrates, NCTA's current proposal would make participation in the market for navigation devices all but impossible for computer industry companies like Dell, HP,

---

[31] *See, e.g.*, NCTA Report at 3-4 (describing various components of the DCAS system, each of which are accessible only through the DCAS Agreement); DCAS Agreement § 2.1 (describing scope of license as covering specifications necessary to produce compliant "host devices"). To the extent that CableLabs use of proprietary technology in the DCAS Agreement excludes manufacturers of certain types of products from the market for cable-compatible navigation devices, the DCAS Agreement may run afoul of the Commission's rules prohibiting cable operators from using their intellectual property to prevent navigation devices from being made available. 76 C.F.R. §§ 76.1201-.1204.

Intel, and Sony. The Companies could, however, support an evenhanded and consumer-driven downloadable security licensing scheme. Such a scheme would differ from that proposed by CableLabs in at least the following ways:

1. **Reasonable Robustness Standards.** Any downloadable software solution to content protection should be based on reasonable robustness standards that allow implementers the freedom to design compliant devices and should not dictate specific implementation details. This type of design flexibility is crucial to creating an environment where innovation flourishes in the development of new means and mechanisms for providing appropriate protection for controlled content. Moreover, allowing design flexibility will permit multi-function platforms like personal computers to participate and innovate in the market for navigation devices and security solutions.

2. **Renewable Software.** Both authentication and decryption functions should be permitted to be implemented through downloadable software. Decryption should not be limited to a hardware implementation, because if the decryption capability or the interfaces to that capability require changes, software implementations could permit a new version to be downloaded to existing products. This could improve the ability of the device to meet defined robustness and compliance rules. Allowing both authentication and decryption to be implemented in downloadable software would have the further benefit of allowing for a more secure and upgradeable integration between the decryption and authentication components. Rules governing the frequency and scope of upgrades to downloadable software could be crafted and included in a revised DCAS license.

3. **Limited and Reasonable Hardware Specifications.** If the cable-compatible DCAS specification must require defined hardware, then the production of those hardware components should be open to all manufacturers under an open standard on nondiscriminatory license terms. Moreover, hardware specifications should be limited and reasonable and should be phased in over a reasonable time period to level the playing field for market entrants. For example, computer manufacturers should not be required to incorporate downloadable security hardware into media processors. Similarly, restrictions on interconnects between internal components of computers should be limited to well-established principles, and the PCI Express interconnect should be explicitly removed from the definition of a "user accessible bus."

   In addition, any hardware requirement should concentrate on providing a secure execution environment for the downloadable software that is performing core content security functions. Hardware requirements should not require implementation of core functions in hardware, which is the end result of the current DCAS license language.

4. **Pre-Adoption Review of DCAS Specification.** If the cable industry wishes to adopt a non-assert licensing framework, it should be willing to share the DCAS specification with potential licensees before they agree not to assert patent claims. Intel has supported patent non-asserts in certain industry-enabling content protection regimes like DTCP and HDCP. These regimes, however, operate on principles of cost recovery, implementation freedom, and self-certification. These licensing schemes are clearly distinguishable from DCAS as currently proposed by NCTA. The relatively narrow non-asserts required by DTCP and HDCP in the interface context, for example, are very different from the wide-ranging non-asserts sought by CableLabs in the complex, IP-rich area of microprocessors. Moreover, unlike DTCP and HDCP, the non-asserts sought by CableLabs directly benefit a proprietary CableLabs technology, and even after the licensee has agreed to the non-asserts included in the DCAS Agreement, CableLabs remains in a position to deny approval of any particular implementation both at the design and the certification level.

5. **Self-Certification.** The Companies acknowledge the cable industry's need to protect the physical integrity of their cable networks, but the change management provisions of the DCAS are simply too strict. Manufacturers should be permitted to make component modifications without being required to submit them to CableLabs for approval. Instead, such changes should be permissible upon the manufacturer's certification that the changes comply with the DCAS specification.

6. **Recognition of Home Networks.** A reasonable downloadable security regime would recognize that once content passes from a permitted output to a legitimate, authenticated device, it is controlled by the user, subject to the digital rights management grant for that content. Multi-function devices must be permitted to distribute content throughout the home network and the downloadable security scheme should recognize and facilitate this distribution so long as that content is output to protected devices.

These changes would lead to a downloadable security regime that encourages broad participation and fair competition among all interested parties.

## V. UNLESS THE CABLE INDUSTRY COMMITS TO TRUE DOWNLOADABLE ACCESS CONTROL, THE COMMISSION SHOULD NOT GRANT ANY FURTHER EXTENSION OF THE DATE BY WHICH THE SECURITY AND DECODING FUNCTIONS OF NAVIGATION DEVICES MUST BE SEPARATED.

The NCTA Report and the DCAS Agreement have been placed before the Commission with the promise that downloadable conditional access can be rolled out nationally by July 1, 2008. To the extent that the cable industry seeks by this roll-out schedule to delay the date by which it is required to separate the security and decoding function of cable navigation

devices beyond the current July 1, 2007 compliance date, the Commission should deny that request. As it currently stands, the NCTA Report and DCAS Agreement provide no basis for the Commission to extend the deadline further.

The point of the Commission's requirement that the cable industry stop producing integrated set-top boxes is to ensure a fully competitive market for cable navigation devices. The downloadable security model proposed by NCTA will have the effect of excluding numerous competitors from that market. It will not achieve the Commission's goal. Moreover, because NCTA's DCAS plan likely will require the use of proprietary CableLabs hardware, the cable industry's current control over the navigation device market will only slightly diminish under the DCAS regime.

We understand that the Commission cannot dictate licensing terms that require the cable industry to make changes to the DCAS Agreement. It can and should, however, inform NCTA that nationwide implementation of DCAS by July 1, 2008 will not discharge the cable industry's obligation to cease selling integrated set-top boxes by July 1, 2007. The Commission also should make clear that it will entertain a modified plan that ensures full participation in the navigation device market by all interested parties willing to comply with reasonable and nondiscriminatory licensing terms. Such terms should require, at a minimum, the changes that the Companies have identified above. Finally, the Commission should urge the cable industry to engage in a public dialogue with all interested would-be manufacturers of cable-compatible navigation devices, so as to arrive at a licensing scheme that would satisfy its separation obligations in the most effective manner. DCAS and the accompanying Agreement, and compliance and robustness rules, were not even considered or developed through CableLabs's typical standards-setting process, which allows input from manufacturers, but instead was issued

by CableLabs as a *fait accompli*. As it has been pointed out in the past, many of the problems with CableLabs licensing regimes – from CHILA to PHILA[32] to DFAST and now to DCAS – could be solved by providing parties that wish to make use of CableLabs licenses a truly open forum and open process to establish true open standards-based specifications and license requirements.

## CONCLUSION

For the reasons stated above, the Companies respectfully request that the Commission issue an Order (1) requiring cable operators to cease selling integrated set-top boxes by July 1, 2007; and (2) permitting NCTA or other cable industry representatives to submit a modified

[32] PHILA is the acronym for the POD-Host Interface License Agreement.

downloadable security proposal that would provide for a truly competitive market for cable-compatible navigation devices.

Respectfully submitted,


**DELL INC.**

/s/ Neeraj Srivastava
Neeraj Srivastava
Director, Client Architecture & Technology
Dell Inc.
One Dell Way
Round Rock, Texas 78682-8033

**HEWLETT-PACKARD COMPANY**

/s/ Adam Petruszka
Adam Petruszka
Director, Strategic Initiatives
Office of Strategy & Technology
Hewlett-Packard Company
2055 State Highway 249
MS-110225
Houston, TX 77070

**INTEL CORPORATION**

/s/ Jeff Lawrence
Jeffrey T. Lawrence
Director, Content Policy and Architecture
Intel Corporation
JF3-147
2111 N.E. 25th Avenue
Hillsboro, OR 97124-5961

**SONY ELECTRONICS INC.**

/s/ Jim Morgan
James Morgan
Director & Counsel
Government & Industry Affairs
Sony Electronics Inc.
1667 K Street, NW
Suite 200
Washington, DC 20006


January 20, 2006