

Law Offices

June 18, 2004

1500 K Street, N.W.  
Suite 1100  
Washington, DC  
20005-1209

Ms. Marlene Dortch  
Secretary  
Federal Communications Commission  
445 Twelfth Street S.W.  
Washington, D.C. 20554

PHILADELPHIA

NEW YORK

LOS ANGELES

SAN FRANCISCO

PRINCETON

HOUSTON

BERWYN

WILMINGTON

Re: Ex Parte of RealNetworks, Inc. MB Docket No. 04-65;  
In the Matter of Digital Output Protection Technology and  
Recording Method Certifications, Helix DRM Trusted Recorder  
and Helix Device DRM Technology

Dear Ms. Dortch:

RealNetworks, Inc. (“RealNetworks”), by its attorneys, hereby submits additional information in support of its pending certification application for interim authorization of Helix Device DRM (Digital Rights Management) Trusted Recorder and Helix Device DRM.<sup>1</sup> This submission is made in response to several issues raised in the course of the RealNetworks meeting with Federal Communications Commission (“Commission”) staff on May 12, 2004. RealNetworks herein clarifies the scope of its interim certification request and provides additional materials in support of its interim certification. RealNetworks is pleased to provide this additional clarification, along with further information related to its Helix Trusted Recorder and Helix Device DRM technology as it relates to the protection of digital output from indiscriminate redistribution, as required by the Commission’s Digital Broadcast Content Protection rules.<sup>2</sup>

<sup>1</sup> In the context of broadcast flag interim certification, “Helix DRM” means the currently commercially-implemented Internet-based use of a Trusted Recorder to distribute content securely. This system has been in wide use for the protection of content distributed over the Internet for over three years. “Helix Device DRM” is a more recent RealNetworks development that contains two software products that can be applied directly in the context of Broadcast Flag digital rights protection: the Helix Trusted Recorder and the Helix Trusted Client.

<sup>2</sup> See Digital Broadcast Content Protection, *Report and Order and Further Notice of Proposed Rulemaking*, MB Docket No. 02-230 (rel. November 4, 2003); 47 CFR §73.9008, Interim Approval of Authorized Digital Output Protection Technologies and Authorized Recording Methods.

Ms. Marlene Dortch

June 18, 2004

Page 2

**Scope of Proposed Interim Certification**

As demonstrated in its interim certification request and in its Reply to Oppositions, Helix Device DRM comply with and, in a number of respects, exceed, the Commission's articulated standards for interim certification. The Helix DRM technology is in use today and its applications include proven and accepted security mechanisms based upon cryptographic technology and computer security that can be, and, with respect to the Trusted Recorder, are being applied to a wide range of consumer devices. While Helix DRM applications possess a range of uses that include restrictions on copying of protected content, in the context of digital broadcast content protection, the Helix DRM and Helix Device DRM technology is highly effective in restricting unencrypted access to protected digital content and is thus highly effective in preventing indiscriminate redistribution of digital broadcast content.

As discussed with the Commission staff, RealNetworks' interim certification filing contained an explanation of a wider range of capabilities for the Helix DRM and the Helix Device DRM than would apply in protecting digital broadcast marked content from indiscriminate redistribution. As reflected in RealNetworks February 27, 2004 Certification ("Certification"), Helix DRM enables a flexible association of a range of possible business rules with valuable media content of all kinds. For purposes of the interim certification, RealNetworks identifies here those portions of the Certification that, in some cases, do not apply directly to the protection of digital broadcast marked content from indiscriminate redistribution.<sup>3</sup>

Specifically, as described in Certification, the Helix Trusted Recorder technology and Device DRM creates an end-to-end DRM solution that allows the protection of digital broadcast marked content ("Marked Content") transmitted across multiple platforms where a Covered Demodulator may be present. Typical instances where a Covered Demodulator may be present include Personal Computers, Set-top Boxes, as well as other devices. Sections 2.1 and 2.2 of the Certification provide a description of Helix DRM generally, which is not directly applicable to Broadcast Flag certification.<sup>4</sup>

---

<sup>3</sup> For example, references in the RealNetworks Certification to CCI states (that is, Copy Once, Copy Freely, Copy No More, Copy Never) apply to the general suite of Helix DRM capabilities and are not applicable to the Commission's Broadcast Flag protection framework, which is not copy-based, but rather, focused on prevention of indiscriminant redistribution of Marked Content.

<sup>4</sup> Also, to the extent RealNetworks Certification submission refers to "content provider" in Section 3.5.3, that description applies only to the more general Helix DRM applications. Implementation of the broadcast flag marked content protection

Ms. Marlene Dortch

June 18, 2004

Page 3

Section 3.4 of the RealNetworks Certification filing provides additional general information about supported rights in general related to the scope of download, playback, transfer and other properties of the overall Helix DRM technology, which has a limited application to the specific Broadcast Flag implementation.

For purposes of ensuring the secure transfer of Marked Content, the Helix DRM Trusted Recorder comes preconfigured with a Trusted Recorder Key. That Key is transferred to the Helix Device DRM Trusted Client using the protocols described in Sections 3.5.4 through 3.5.6 of the Certification request. As explained in the Certification, the Trusted Recorder will be located on the Covered Demodulator product. This Trusted Recorder interfaces with the Trusted Client to validate the accessibility for playback and further distribution of the Marked Content by the exchange of Keys that allows for the de-encryption of Marked Content. Necessary licenses for consumption of Marked Content will be stored on the Trusted Recorder, and they, together with the Key database, form the core of protection of Marked Content from indiscriminate redistribution. For purposes of this digital broadcast Marked Content protection regime, the Trusted Recorder is protected by the same tamper resistance techniques described in Section 3.2.4 of the RealNetworks' Certification for Helix DRM and Helix Device DRM.

The Trusted Client is responsible for seeking and obtaining the license to access unencrypted Marked Content when it seeks to obtain a copy of the secure media file from a Trusted Recorder. As an example, a set-top box would use universal plug and play capability to discover Marked Content on a PC server that contains a Covered Demodulator. This process of content discovery occurs by technology devices on a home network browsing content repositories on various machines and discovering Marked Content. As discussed further herein, RealNetworks will apply proximity controls, such as Round Trip Time ("RTT") and Time to Live ("TTL"). Thus, the Trusted Recorder would handle the testing of the RTT and TTL, and only allow the transfer of the Trusted Recorder Key if the Trusted Client passes the relevant tests. The user application on the set-top box would then handle the communications between the Trusted Recorder and the Trusted Client. Once the license transfer is complete, the set-top box would download or stream the Marked Content from the PC server.

The Trusted Recorder and Trusted Client have more than a single means to allow the Trusted Client to access the Trusted Recorder to request unencrypted access to Marked Content. A Trusted Client can also access Marked Content validated by the

---

requirements does not require the direct involvement of any content providers – the Commission's rules effectively act as a surrogate mechanism to protect content owners' interests.

Ms. Marlene Dortch

June 18, 2004

Page 4

Trusted Recorder over other means, including via the Internet. In that and any other case, and with other classes of devices, any device receiving Marked Content would be treated by the Trusted Recorder as a Trusted Client. In every case the Trusted Recorder must authenticate the Trusted Client before the Trusted Client can access Marked Content in any usable manner. As described above, the Trusted Recorder handles the testing of the RTT and TTL, and only allows the transfer of the Trusted Recorder Key if the Trusted Client passes the relevant tests. If a downstream device does not have the ability to function as a Trusted Client, Helix Device DRM will authenticate and download Marked Content only to those devices that have Commission-approved digital output protection technology once an agreed-upon method for mutual recognition is developed.

### **Robustness**

The Commission's basic standard for robustness requires that content protection be implemented in a reasonable manner, so that it cannot be defeated by generally-available tools or equipment.<sup>5</sup> Helix Trusted Recorder today is in wide use as a viable method of protecting high value content from indiscriminate copying, playback and distribution by the use of cryptographic exchange of keys between the Trusted Recorder and the Trusted Client.

Given the importance to content owners of protecting their valued content, RealNetworks has, on two occasions, had separate outside auditors review the cryptographic implementation and applications within the Helix DRM. In July of 2001, Telcordia performed an audit and in January 2002, Merdan performed an audit. Notably, both audits found that the Helix DRM application of cryptography was appropriate and accomplished the Digital Rights Management goals of the system.

Given its strong encryption standards, Helix Device DRM cannot be defeated using generally available tools or equipment. In the event of any potential breach or compromise of the Helix Device DRM in the context of Broadcast Flag, the effect would be extremely limited and very local. Specifically, if a particular device is breached, (*i.e.*, the security has been compromised so that Marked Content distributed to a device or an application resident on the device is altered to defeat the Marked Content protection) the extent of the breach is contained to that particular device, as well as potentially to the content on that device. Thus, even if devices with Helix Device DRM in fact were to be compromised by end user intervention, that situation would not create an avenue for breach or attack on any Helix Device DRM upstream devices. In other words,

---

<sup>5</sup> See 47 C.F.R § 73.9007 – Robustness Requirements for Covered Demodulator Products.

Ms. Marlene Dortch  
June 18, 2004  
Page 5

compromise of a downstream device will not compromise the ability of any upstream component of Helix Device DRM to continue to protect Marked Content from indiscriminate redistribution. As demonstrated in RealNetworks Certification and Reply to Opposition, in no instance can a compromised Trusted Client be used to validate and permit unencrypted access to Marked Content from a Trusted Recorder.

### **Revocation and Renewability**

RealNetworks Helix Device DRM is a flexible mechanism that allows for control of the revocation of rights to access Marked Content as described in its Certification and as more specifically articulated in RealNetworks Reply to Opposition.<sup>6</sup> In the Certification and Reply, RealNetworks demonstrated that the Helix Device DRM can provide for revocation capabilities both at the content level (*e.g.*, content can no longer be consumed) and the component level (*e.g.*, the Helix applications cannot be rendered). This range of capabilities exceeds Commission requirements, which require information regarding only device level revocation. Given the manner in which Helix encryption of Marked Content is associated with only a single Trusted Recorder Key, the revocation of a Trusted Recorder Key results in all Helix Device DRM encrypted Marked Content files associated with that Trusted Recorder Key becoming unusable.<sup>7</sup>

In the event that RealNetworks has reason to believe that a Helix Device DRM application – either a Helix Trusted Recorder or a Helix Trusted Client -- itself is insecure, breached, or no longer authorized to access Helix Device DRM encrypted Marked Content, component revocation can be invoked. More particularly, RealNetworks may make that determination when RealNetworks has reason to believe that a secret symmetric key or private key associated with a Trusted Client certificate has been lost, stolen, intercepted or otherwise misdirected or made public or disclosed. Additionally, and as provided in the License Agreement previously provided to the Commission, in the event that RealNetworks has reason to believe that a licensed distributor is in breach of the license agreement (including, particularly, breaches relating to implementation of robustness or security requirements promulgated by the Commission or by RealNetworks), RealNetworks may revoke the Helix Device DRM on the relevant devices. Revocation can take place with respect to a single device, a class of device, or an application, and may be accomplished either through distributing

---

<sup>6</sup> RealNetworks Reply to Opposition at 7-10.

<sup>7</sup> Further, as discussed in its Reply, whenever devices connect to a Helix Device DRM that contains a list of Trusted Recorder Keys, those revoked Trusted Recorder Keys will be transmitted to the connecting device and will render the revoked Marked Content unplayable on that device. Reply at 8.

Ms. Marlene Dortch

June 18, 2004

Page 6

information concerning revoked certificates through protected content delivered via the Internet or any other digital network through which the relevant device is connected, or through physical media. A revoked device may be renewed through a software upgrade correcting the relevant security problem. Such upgrade may be distributed via the Internet or any other digital network through which the device is connected, or through distribution of the upgrade on physical media. The distribution license for the Helix Device DRM requires licensed distributors to distribute upgrades, and to cease distribution of older versions of the Helix Device DRM when upgrades are provided. This capacity for revocation and renewal via upgrade distribution provides a flexibility that protects content owners (through the ability to respond rapidly to a security breach) and to consumers and device manufacturers (ensuring, as much as possible given the nature of the particular device, a rapid renewal).

Each and every Trusted Recorder and Trusted Client includes a secure database containing revoked components and each component of the Helix Device DRM includes a unique digital signature stored in the component itself. Each time playback is initiated, the Helix Device DRM authenticates the signatures of all components that will handle decrypted data using a secure database of revoked signatures. If a digital signature appears in the database, the component will fail validation and playback until that component is renewed.<sup>8</sup>

RealNetworks agrees with certain other parties that have pending certification requests that it is inappropriate at this time to provide a formal process for a particular category of content to determine the appropriateness of revocation. RealNetworks believes that the strength of a software-based solution is the rapidity with which both revocation and renewal can occur, and such strength should not be compromised by a process that requires third parties to be heard before revocation can occur. However, if required by the Commission, RealNetworks would incorporate a formal process for revocation in its license agreements with licensed distributors of the Helix Device DRM.

RealNetworks agrees with other parties that have pending certifications that there is a need for interoperable or open methods for recognizing and delivering revocation messages. In the RealNetworks April 16 Reply, RealNetworks stated that it was open to

---

<sup>8</sup> Helix Device DRM AutoUpdate technology allows the secure delivery of software updates. If a component fails, AutoUpdate is loaded and a request is made to an Internet-based AutoUpdate server. Assuming there is a new component available to address the security issue, the new component is downloaded, verified and installed without the need for end user intervention. For offline scenarios, renewability also can occur through firmware updates from device manufacturers.

Ms. Marlene Dortch

June 18, 2004

Page 7

standardizing a method or methods to deliver revocation information within the digital broadcast transport stream that could be recognized and acted upon by all downstream devices. RealNetworks supports interoperability for purposes of propagating revocation messages to all downstream devices. This interoperability should extend to all devices capable of any Broadcast Flag certification system. To have a fully interoperable revocation capability, the Commission should consider the need to create a certification registry or some similar functionality, so that all entities capable of cooperation can cooperate to ensure all devices can react appropriately to a revocation message.

### **Licensing of Technology and Implementation**

Once certified by the Commission as an interim authorized digital content protection method, RealNetworks will make its Helix Device DRM software available to device manufacturers through reasonable and non-discriminatory license agreements, consistent with RealNetworks existing practices. RealNetworks attached its proposed licensing agreement to its Reply to Opposition for the Commission to evaluate the transparency of the license terms.

As other certification applicants have observed, the Commission's requirement of "reasonable and non-discriminatory" licensing has no single, standard bright line definition associated with it.<sup>9</sup> Using a common sense approach, RealNetworks suggests that, for RealNetworks Certification, the Commission's requirement reflects a concern that all similarly situated potential licensees have access to the Helix Device DRM technology and implementation on the same terms and conditions. The RealNetworks license agreement submitted as part of the Certification process meets this standard.

To the extent that the Commission deems "reasonable" to be any form of judgment regarding the availability of a license at cost levels that do not undermine the economic model for digital broadcasting, RealNetworks can confirm that its compensation for licensing Helix Device DRM for Broadcast Flag will encourage the availability of low cost devices. Under the terms of the license agreement, all licensing compensation to RealNetworks will be structured solely as a per unit royalty arrangement, which is a predictable and stable framework. Any forward-looking changes to the licensing agreement also will be made on a reasonable and non-discriminatory basis.

---

<sup>9</sup> See Reply of the Digital Transmission Licensing Administrator LLC, Supporting Certification of DTCP, filed April 16, 2004 in MB Docket No. 04-64 at 14.

Ms. Marlene Dortch

June 18, 2004

Page 8

### **Proximity Requirements**

As RealNetworks observed in its April 16, 2004 Reply to Opposition, there is nothing in the Commission's interim authorization rules that requires the implementation of any form of proximity control.<sup>10</sup> However, RealNetworks recognizes that its Helix Device DRM technology expressly allows delivery of the Trusted Recorder key to Trusted Clients to access Marked Content over the Internet, and this fact raised an effectiveness concern for the MPAA. Specifically, the MPAA and the studios filing with it expressed concern that there would be no effective form of protection of Marked Content outside of the personal digital network environment ("PDNE") that the Commission is considering adopting in the context of permanent authorizations for the protection of Marked Content.<sup>11</sup>

Despite the fact that there is no proximity control requirement in the Commission's interim authorization rules, RealNetworks understands that proximity controls is a crucial issue for the MPAA parties.<sup>12</sup> As stated in its Reply to Opposition, there are certain measures that can be taken in an attempt to simulate a physical proximity limitation, including the encoding of a TTL instruction.<sup>13</sup> There are further techniques, such as applying an RTT parameter to mimic the scope of redistribution that content would likely have within a personal digital network environment. RealNetworks will commit to use both TTL and RTT in its Broadcast Flag implementation. RealNetworks is in active discussions with the MPAA regarding implementation specifics and other possible forms of proximity limitations it could employ. RealNetworks will inform the Commission immediately upon the completion of these discussions.

### **Conclusion**

As demonstrated herein, RealNetworks' Helix DRM and Helix Device DRM are readily adaptable for use as a means to protect Broadcast Flag Marked Content from

---

<sup>10</sup> RealNetworks Reply to Opposition at 6-7.

<sup>11</sup> MPAA Parties Opposition at 3-7.

<sup>12</sup> The MPAA recently endorsed the Thomson SmartRight Certification due to its decision to implement RTT and TTL technologies. See joint MPAA/Thomson *ex parte* letter, filed May 28, 2004, in MB Docket No. 04-59.

<sup>13</sup> RealNetworks Reply to Opposition at 6-7.

Ms. Marlene Dortch  
June 18, 2004  
Page 9

indiscriminant redistribution. Pending a final decision on the scope of proximity controls that RealNetworks can adopt, RealNetworks submits that its Helix DRM and Helix Device DRM technology and the associated licensing are consistent with Commission requirements, and indeed exceed the Commission's articulated standards for certification. Accordingly, RealNetworks seeks certification on an interim basis for its Helix DRM and Helix Device DRM application.

Respectfully submitted,



Laura H. Phillips  
Counsel for RealNetworks, Inc.

cc: Steven Broeckaert  
Rick Chessen  
John Gabrysch  
Alison Greenwald  
Amy Nathan  
Jeffrey Neumann  
Susan Mort  
Mary Beth Murphy  
Alan Stillwell