

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

_____)
)
In the Matter of)
)
Digital Output Protection Technologies)
and Recording Methods Certifications)
)
TiVoGuard Digital Output Protection)
Technology)
_____)

MB Docket No. 04-63

**REPLY OF TIVO INC. TO THE OPPOSITION OF THE MOTION PICTURE
ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS
INC., PARAMOUNT PICTURES CORPORATION, SONY PICTURES
ENTERTAINMENT INC., TWENTIETH CENTURY FOX FILM
CORPORATION, UNIVERSAL CITY STUDIOS LLP, THE WALT DISNEY
COMPANY, AND WARNER BROS. ENTERTAINMENT INC.**

Matthew Zinn
General Counsel

Max P. Ochoa
Corporate Counsel

TiVo Inc.
2160 Gold Street
Alviso, CA 95002-2160

James M. Burger
Briana E. Thibeau

Dow, Lohnes & Albertson, PLLC
1200 New Hampshire Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 776-2300

Its Attorneys

April 16, 2004

TABLE OF CONTENTS

	Page
SUMMARY	i
I. INTRODUCTION	1
II. TIVO’S PROPOSED PROCEDURES AND TECHNOLOGY PROVIDE BETTER SECURITY THAN THOSE PROPOSED BY THE MPAA PARTIES, GIVE EFFECT TO THE BROADCAST FLAG, AND SHOULD BE APPROVED AS TO TIVO® DVRS	2
A. Any Downstream Device Manufactured, Sold, or Distributed by TiVo Will Adhere to the Broadcast Flag Compliance and Robustness Requirements Set Forth in the Commission’s Rule.....	3
B. The MPAA Parties’ Request for a Formal Private Role in TiVo’s Revocation, Renewal, and “Change Management” Procedures Is Unnecessary and Unreasonable	4
1. The MPAA Parties’ Requests Are Unnecessary as Content Owners Already Have Adequate Forums for Any Concerns They May Have About the Security of TiVo’s System, and TiVo Has Every Incentive to Maintain That Security	4
2. The MPAA Parties’ Requests Are Unreasonable in That Granting Private Contractual Rights to Content Owners Would Result in Time-Consuming Negotiations, Would Place the Security of Technologies at Risk, and Would Be Unprecedented	8
C. A Grant of Third-Party Beneficiary Rights to Content Owners Is Beyond the Commission’s Scope of Authority and Would Constitute an Unlawful Delegation of the Commission’s Authority.....	12
D. The TiVoGuard Technology Does Not Place Any Obligation on Content Owners, Broadcasters or Others	17
E. The MPAA Fails to Raise any Objections to the Ability of TiVoGuard to Give Effect to the Broadcast Flag and, Therefore, the Commission Should Approve TiVo’s Certification as to Standalone Devices.....	17
III. TIVO’S PROPOSED PROCEDURES AND TECHNOLOGY FOR “TIVOTOGO” GIVE EFFECT TO THE BROADCAST FLAG AND SHOULD BE APPROVED BY THE COMMISSION	18
A. TiVo’s PC Implementation Is Secure and Satisfies the Compliance and Robustness Requirements of the Rule	18
B. The Distance Limitation Proposed by the MPAA Parties Is Outside the Scope of the Interim Rules and the Commission’s Determinations in this Proceeding	19

TABLE OF CONTENTS
(continued)

	Page
IV. CONCLUSION.....	24
ATTACHMENT A - TIVOTOGO PERSONAL COMPUTER SUPPLEMENT	1

Summary

In their Opposition to TiVo's certification ("Certification") seeking interim authorization of its TiVoGuard technology, the MPAA Parties attempt to raise various system administration and compliance issues that relate to both standalone TiVo[®] products and "TiVoToGo" PC implementations of TiVo's "TiVoGuard" security system. The MPAA Parties also attempt to raise issues relating to system security and scope of redistribution that relate only to TiVoToGo. These objections are unfounded. None of the MPAA Parties' objections go to the heart of the Commission's broadcast protection requirement. TiVoGuard's strong security system gives effect to the broadcast flag. In addition, TiVo's system administration procedures provide far better security than would the revocation, renewal, and change procedures proposed by the MPAA Parties. While TiVo is willing to make minor clarifications regarding its system administration procedures, it finds no merit in the balance of the MPAA Parties' objections.

By way of clarification, TiVo affirms that it will adhere to the broadcast protection Compliance and Robustness Requirements with respect to any downstream device it manufactures, sells, or distributes and will similarly require its licensees to adhere to these obligations. However, with regard to the MPAA Parties' unprecedented request for a formal, quasi-regulatory role in TiVo's revocation, renewal, and change decisions, TiVo submits that there is no reasonable basis for granting that request. TiVo has adequate incentives to maintain the security of its own system, and any failure to do so should be adjudicated by the Commission, not content owners. The MPAA Parties' request for third-party beneficiary rights likewise is unreasonable, unprecedented, and would constitute an unlawful delegation of the Commission's authority. Finally, TiVo

represents that its system places no obligations on content providers, broadcasters, and others who only use the broadcast flag to invoke the protections of the TiVoGuard system, or on consumers who merely transmit or receive marked content. As the MPAA Parties take no issue with respect to the security of standalone TiVo devices and their ability to give effect to the broadcast flag, and the Parties' concerns regarding scope of redistribution are moot as regards the standalone devices, the Commission should readily approve TiVo's Certification with respect to TiVoGuard for its standalone digital video recorders ("DVRs").

The Commission also should approve TiVo's Certification with respect to TiVo's PC implementation – TiVoToGo – as TiVoToGo satisfies the Compliance and Robustness Requirements set forth in the Commission's Rule. Rejecting TiVo's Certification with respect to its PC implementation on the basis of the MPAA Parties' security concerns would be tantamount to excluding PCs from the DTV transition. The MPAA Parties' "proximity of redistribution" concerns delve into matters the Commission has expressly placed outside the scope of this proceeding. Additionally, the Parties' "proximity of redistribution" concerns are misplaced, as TiVo's "secure viewing group" feature restricts the indiscriminate redistribution of marked and unscreened content. Therefore, these concerns should be given no weight by the Commission in evaluating TiVo's Certification. The Commission should approve TiVo's Certification of its standalone devices and the TiVoToGo PC implementation.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

_____)
)
In the Matter of)
)
Digital Output Protection Technologies)
and Recording Methods Certifications)
)
TiVoGuard Digital Output Protection)
Technology)
_____)

MB Docket No. 04-63

**REPLY OF TIVO INC. TO THE OPPOSITION OF THE MOTION PICTURE
ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS
INC., PARAMOUNT PICTURES CORPORATION, SONY PICTURES
ENTERTAINMENT INC., TWENTIETH CENTURY FOX FILM
CORPORATION, UNIVERSAL CITY STUDIOS LLP, THE WALT DISNEY
COMPANY, AND WARNER BROS. ENTERTAINMENT INC.**

TiVo Inc. (“TiVo”) hereby submits this reply to the opposition (“Opposition”) filed by the Motion Picture Association of America, Inc. (“MPAA”), Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLP, The Walt Disney Company, and Warner Bros. Entertainment Inc. (collectively, “the MPAA Parties” or “the Parties”) against TiVo’s certification (“Certification”) seeking interim authorization of its TiVoGuard technology.

I. Introduction

TiVo appreciates the MPAA Parties’ positive characterization of TiVo’s “TiVoGuard” digital output protection technology and the Parties’ recognition of

TiVoGuard's strong security, upgradeability, revocability, and renewability features. However, TiVo rejects the MPAA Parties' assertion that TiVo's Certification has "serious omissions."¹ The MPAA Parties raise numerous objections in their Opposition regarding the sufficiency of TiVo's Certification, but the Parties' objections are unfounded. These objections generally fall into two categories. The first category consists of complaints about TiVo's administration of the TiVoGuard system and TiVo's mechanisms for ensuring that downstream devices comply with the Commission's Rule.² These arguments relate to both standalone TiVo products and "TiVoToGo" PC implementations of TiVoGuard. The second category relates only to PC implementations of TiVoGuard and consists of concerns about TiVoToGo's security and its scope of redistribution of marked and unscreened content. While TiVo is willing to make certain minor clarifications regarding its system administration procedures, it finds no merit in the MPAA Parties' objections and sees no reasonable basis for the Commission to reject its Certification. As TiVo's Certification demonstrates, TiVo's digital output protection technology provides a level of security that is appropriate for use in covered demodulator products to give effect to the broadcast flag. Therefore, TiVo's Certification should be approved both for TiVo's standalone devices and for its TiVoToGo PC implementation.

II. TiVo's Proposed Procedures and Technology Provide Better Security Than Those Proposed by the MPAA Parties, Give Effect to the Broadcast Flag, and Should Be Approved as to TiVo® DVRs

TiVo's system administration procedures are appropriate and in fact provide better security than would the revocation, renewal and change procedures proposed by

¹ See Opposition at 3.

² See *Digital Broadcast Content Protection, Rule*, MB Docket No. 02-230, 68 Fed. Reg. 67599, at §§73.9003 – 73.9007 (released December 3, 2003) ("Rule").

the MPAA Parties.³ Nonetheless, TiVo is willing to make certain minor clarifications regarding these procedures, as described below. TiVo submits, however, that the MPAA Parties' requests for a formal, private, and/or contractual role in revocation, renewal, and change procedures, and for third party beneficiary rights in private agreements, are unreasonable, unnecessary, and inappropriate in the context of the Commission's proceeding.

A. Any Downstream Device Manufactured, Sold, or Distributed by TiVo Will Adhere to the Broadcast Flag Compliance and Robustness Requirements Set Forth in the Commission's Rule

As the MPAA Parties correctly point out, the Commission's Rule does not directly require devices that operate downstream of a covered demodulator product to comply with the Compliance and Robustness Requirements set forth in the Rule. The Parties assert in their Opposition that TiVo must therefore provide assurances that content protection obligations will persist in any downstream device that incorporates the TiVoGuard technology. As TiVo explained in its Certification, all TiVo devices, whether built by TiVo or its licensees, are built to TiVo's rigid and thorough specifications,⁴ which far exceed the broadcast protection Compliance and Robustness Requirements. Nonetheless, TiVo affirms to the Commission that it will adhere to the broadcast protection Compliance and Robustness Requirements with respect to any downstream device it manufactures, sells, or distributes. TiVo further affirms that it will amend any TiVoGuard license granted to downstream product manufacturers to contractually obligate the manufacturers to design and build such devices in accordance

³ See Opposition at 8, 10.

⁴ See Certification at 33.

with the Compliance and Robustness Requirements contained in Sections 73.9003 through 73.9007 of the Commission's Rule.

B. The MPAA Parties' Request for a Formal Private Role in TiVo's Revocation, Renewal, and "Change Management" Procedures Is Unnecessary and Unreasonable

The MPAA Parties argue that TiVo's Certification should be rejected because TiVoGuard "does not provide content owners any role" in requesting device revocation and system renewal or objecting to changes in TiVo's technology.⁵ The contention that content owners should have any role in these areas beyond that provided in the Rule⁶ is unfounded. More importantly, discussion of this issue is moot, as TiVo's technology satisfies the articulated standards for interim approval – it gives effect to the broadcast flag. Nonetheless, assuming *arguendo* that it is appropriate for the Commission to consider the MPAA Parties' demands, the Commission should reject these demands as unnecessary and unreasonable.

1. The MPAA Parties' Requests Are Unnecessary as Content Owners Already Have Adequate Forums for Any Concerns They May Have About the Security of TiVo's System, and TiVo Has Every Incentive to Maintain That Security

The Commission – not any content owner – is the appropriate arbiter of complaints about the sufficiency of a particular technology under the Rule. Nowhere in its Report and Order⁷ or Rule does the Commission require proponents of digital output protection technologies to separately negotiate with and provide contractual rights to content owners. On the contrary, the Commission developed its broadcast protection rules at the behest of the content owners to provide for a federal regulatory scheme that

⁵ See Opposition at 8, 10.

⁶ See Rule at §73.9008(e).

⁷ *Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rulemaking*, MB Docket No. 02-230, (released November 4, 2003) ("Report and Order").

would obviate the need for private negotiation in this area. Now, having asked for and received a federal regulatory scheme to regulate DTV demodulators, it appears that the MPAA Parties are asking the Commission to create a parallel *private* regulatory scheme so that content owners may make their own determinations as to a particular technology's adequacy under, or compliance with, the FCC's Rule. This is unnecessary and wholly inappropriate given that the Commission's Rule already provides a forum for persons who believe that the security of a particular content protection technology or recording method has been compromised.⁸ In the event that a content owner believes that TiVoGuard has been compromised, or that the Commission's Rule has been violated, it may file a complaint with the Commission and have that complaint reviewed in a fair and impartial manner.⁹ In addition, as more fully discussed in Section III(B) below, the content owners may avail themselves of the Copyright Office and the courts to enforce their rights under the Copyright Act.

Moreover, it is both adequate and appropriate for decisions about revocation, renewal, and change to rest first and foremost with technology providers, and there is no reason to doubt their commitment to maintaining the standards of the Commission's Rule. While the MPAA Parties assert that leaving revocation, renewal and change procedures in the hands of TiVo alone is "inadequate,"¹⁰ such as assertion unfounded. Revocation, renewal, and change management are extremely sensitive issues that, if handled poorly, have the potential to seriously disrupt use by consumers and manufacturers of digital broadcast protection technologies and slow the transition to DTV. Unnecessary

⁸ See Rule at §73.9008(e).

⁹ While, as noted *infra*, TiVo encourages any content owner to advise TiVo when it believes it has found an inadequacy in the TiVoGuard system, this is distinct from invading private contracts and demanding that the FCC provide content owners extra-regulatory authority.

¹⁰ Opposition at 8.

revocation of consumer devices will disrupt consumers' ability to enjoy DTV programming and make consumers wary of investing in DTV products. Moreover, if technology providers are unable to make timely repairs or changes, innovation, system security, and product cost will be negatively impacted and the transition to DTV may be hindered.

The MPAA Parties suggest that, unless they are given the right to directly request revocation, renewal, or change to TiVo's security system, system compromises will go unnoticed and/or uncorrected.¹¹ The MPAA Parties are simply wrong when they assert that "TiVo may have little practical incentive to identify, investigate, and take action against compromised device keys or identity certificates."¹² On the contrary, TiVo has *every* incentive to revoke devices or renew or change its system as necessary to ensure that content is adequately protected. As TiVo explained in its Certification, TiVo's interests are uniquely different from those of other technology providers that primarily are hardware vendors, because TiVo's business model wholly depends upon the maintenance of TiVoGuard's integrity.¹³ Without the exclusive ability to activate and deactivate the TiVo[®] service on TiVo devices, TiVo exposes its service to piracy and jeopardizes its revenue stream. Similarly, without the ability to quickly upgrade or repair its system, TiVo risks compromising consumer privacy and, in turn, consumer confidence. Any breach of TiVo system security could threaten TiVo's vital business interests and continued viability as a company. That very same system is used to secure content via TiVoGuard. It bears repeating – while a compromise of TiVo's security system could put digital content at slightly greater risk of piracy, it would definitely present a

¹¹ *Id.*

¹² Opposition at 8.

¹³ TiVo Certification at 9-10.

significant threat to TiVo's business model and reputation with its customers and the general public. Thus, TiVo's incentives are more than adequate to ensure the continued security of the TiVo system and of digital broadcast content.¹⁴ It is wrong for the MPAA Parties to characterize TiVo's interest in protecting its own business model as an inadequate incentive to maintain the security of its system, while simultaneously asserting the protection of their own business model as a justification for giving them a formal, private, and quasi-regulatory role in the administration of the TiVo system.¹⁵

In fact, TiVo's own business incentives have given rise to more than adequate revocation and renewal procedures. TiVo has a privacy and security department that is devoted to protecting user privacy and preserving the integrity of the TiVoGuard system. TiVo welcomes information from content owners and other parties about potential compromises to its system. Given the importance of security to TiVo's business, it is highly unlikely that TiVo would ignore a report of a serious breach or compromise to its system, even absent the formal role the MPAA Parties request. In the face of a serious

¹⁴ In fact, unlike certain content owners that have the luxury of making an economic decision to not protect their higher-volume releases, TiVo's own business incentives demand that it not allow the security of content to be compromised. See Jon Healey, *Taking Different Tacks on Piracy*, Los Angeles Times (Oct. 15, 2003), available at <http://www.latimes.com/technology/la-fi-matrix15oct15224419.1.2898731.print.story?coll=la-headlines-technology> (last visited April 16, 2004); Barry Fox, *Harry Potter Released Unprotected*, NewScientist.com (June 13, 2003), available at <http://www.newscientist.com/news/news.jsp?id=ns99992404> (last visited April 16, 2004); Gwendolyn Mariano, "Harry Potter" DVD Protection Goes Poof, News.com (June 20, 2002), available at <http://news.com.com/2100-1023-938008.html> (last visited April 16, 2004).

¹⁵ Even if a technology provider did not have as great an incentive as does TiVo to protect the integrity of its system, the MPAA Parties' arguments only support the conclusion that they should not have an independent formal role in content protection system administration. The MPAA Parties, at their own insistence, have no financial responsibility for the content protection systems. As noted (see note 20 *supra*), they want the FCC to ensure they do not have to pay for any technology provider's intellectual property used to protect their own intellectual property. Also, the standard the FCC has adopted for broadcast content protection is a speed bump, not unachievable perfect protection. Since the MPAA Parties' investment in the content protection system is zero, as is the cost to them of any change, their incentive is to demand a higher level of protection than necessary. Accordingly, the FCC must maintain its independent role to balance the various interests with the goal being a successful DTV transition, rather than delegating their authority to private parties, which if left to their own devices, would demand perfect protection at any price – as long as it's on someone else's dime.

breach, however, TiVo needs the ability to respond quickly, without having to submit to a time-consuming private review, approval, and arbitration process. The current TiVoGuard system can readily revoke or renew devices. Unlike any other proposed technology, TiVoGuard automatically revokes a TiVo device if it fails to “report in” to TiVo’s server. It is hard to imagine how the MPAA Parties could deem an automatic revocation system “inadequate.”

2. The MPAA Parties’ Requests Are Unreasonable in That Granting Private Contractual Rights to Content Owners Would Result in Time-Consuming Negotiations, Would Place the Security of Technologies at Risk, and Would Be Unprecedented

As noted above, the MPAA Parties assert that they should be given a formal, private role in TiVo’s revocation, renewal and change procedures, despite the fact that the Parties asked the *Commission* to regulate TiVo’s technology. In particular, the MPAA Parties complain that TiVoGuard “has no provision for ‘Change Management,’ that is, a procedure under which content owners have a meaningful opportunity to object to changes in the technology.”¹⁶ The term “Change Management,” however, does not appear anywhere in the Commission’s Report and Order or in the Rule. Instead, the Rule contemplates only that a technology provider will certify that its technology complies with the Rule.¹⁷ A technology provider presumably will be in violation of the Rule if it makes any change to its system that causes its system to fall out of compliance with the Rule. If that happens, the MPAA Parties are free to file a complaint with the Commission.¹⁸ In the case of TiVo’s technology, the MPAA Parties will have ample notice of any security changes made to the TiVo system. As TiVo stated in its

¹⁶ Opposition at 10.

¹⁷ See Rule at §§73.9008(a), (c).

¹⁸ See Rule at §73.9008(e).

Certification, TiVo will notify the Commission of any security changes made to the TiVoGuard system.¹⁹

The MPAA Parties appear to suggest that the Commission should mandate private negotiations between technology providers and content owners anytime that any revocation, upgrade, repair, or change is necessary.²⁰ With regard to changes in technology, the MPAA Parties appear to propose that, by private contract, every protection technology vendor should submit “any proposed changes” to all content providers under an undefined “Content Participant Agreement.” This novel proposal is problematic in many respects.

First, if the Commission grants the MPAA Parties the private rights they are requesting, those rights will be subject to arms-length negotiations between each technology proponent and each content provider. The process to negotiate those rights would be time-consuming and would place the security of approved technologies at risk. It took three years for the Digital Transmission Licensing Administrator (“DTLA”) and the MPAA Parties to negotiate a “Content Participant Agreement,” and, to TiVo’s

¹⁹ Although not required by the Rule, in its Certification TiVo committed to the following: “In the event that TiVo deems it necessary or prudent to modify or renew its security mechanisms (*e.g.*, in the event of a system compromise or advances in cryptanalysis), TiVo will notify the Commission of the different security mechanism(s) employed and will ensure that any such changes are made within the framework of the Rule.” TiVo Certification at 31.

²⁰ The MPAA Parties, collectively or individually, may have participated in the content protection market by developing and/or investing in other content protection technologies but they have never offered to buy, license, or fund TiVoGuard technology. Indeed, both with respect to individual Certification applications and in the Broadcast Protection Proceeding, the MPAA Parties have clearly stated their position – they demand assurance that they will not have to spend a single cent on systems designed solely to protect their intellectual property. Opposition at 10-11. *See also*, Reply Comment of DTLA in MB Docket No. 02-230 (filed March 15, 2004) at 8: “... DTLA does not mean to suggest that other technology proponents must follow DTLA’s chosen model, or that content owners should not have a responsibility to pay for protecting their content. Technology companies should be under no obligation to provide rights to their intellectual property for free just so content owners can charge for theirs.” Accordingly, it is unreasonable for the MPAA Parties, in effect, to petition the government to establish a Federal regulatory scheme and then to insist the government interfere with private contractual rights by delegating authority to the MPAA Parties to act as a private FCC regulatory body.

knowledge, only two studios have even signed the agreement. Also, while that agreement may have clauses that DTLA believes are a reasonable bargain for granting revocation, upgrade, repair, or change approval rights, no other technology proponent was a party to those negotiations. Therefore, each technology proponent will have to engage in its own negotiations with all content owners²¹ and will have to hope that they have better results than DTLA when it comes to persuading the MPAA Parties, as well as the other content owners, to sign. It is not unreasonable to imagine years of negotiations taking place with only marginal benefits, if any, to consumers, content owners, or technology providers at the end of the day.

Second, technology providers may want to make minor changes to their technologies that are unrelated to the Compliance and Robustness Requirements and/or do not have a material impact on the technology's compliance with those requirements. It would be unreasonable and unnecessary to require such changes to be submitted to the Commission, content owners, or any other party. Moreover, there may very well be circumstances where, to protect the security of a system, material changes need to be

²¹ Another problem inherent in the MPAA Parties' demand is their failure to recognize that they represent only a portion of all copyrighted video transmitted on DTV. It should be noted that the National Association of Broadcasters, for example, demanded that local news programs be protected as important copyrighted material. *Ex Parte* Letter (with attachments) filed by the National Association of Broadcasters, MB Docket 02-230 (Oct. 27, 2003): "It is particularly important that the protection of the broadcast flag apply to all programming on broadcast stations, and thus we oppose any exemption for local news and public affairs programs. Those programs are the major product of local television stations. Their copyright interest in those programs is the same as the interest that program producers have in any other type of program, and local stations should similarly be protected against unauthorized redistribution of their intellectual property."

The MPAA Parties have not represented that they have negotiated a power of attorney from the more than 1,600 independent DTV broadcasters, and all other creators of copyrighted content displayed on DTV, giving them the power to exercise all the rights they demand from the FCC. TiVo is not aware of any such transfer of power to the MPAA Parties. Accordingly, if the FCC withheld certification until all technology providers negotiated the rights demanded by the MPAA Parties (and all seven studios were willing to sign a Content Participant Agreement) and even if the technology providers were willing enter into FCC mandated negotiations with all DTV copyright holders, no technology would ever be certified.

made and made quickly.²² In these cases, the only practical “reporting” would be after the fact.

Third, adding a layer of private contract negotiations between technology proponents and the Commission will do nothing to reinforce content protection. On the contrary, it may hinder protection in circumstances where maintenance of security calls for swift action as noted above. It also would add unnecessary expense and slow innovation to a crawl. Private negotiations are time-consuming, would only place the security of approved technologies at greater risk, and are unnecessary in light of other remedies available to content owners. Even if the FCC could craft a reasonable way of mandating negotiations between all the content owners and all the technology proponents, it is simply unnecessary. The technology proponents that have filed certification applications with the Commission are all well-respected corporations that do not need direct supervision by *both* the content owners and the FCC.

Finally, providing content owners with a formal, private role in the administration of the TiVoGuard system would be unusual. Such private contractual rights are rarely provided by the Commission to third parties when a party otherwise subject to the FCC’s rules violates those rules. Moreover, as discussed in the next section, the grant of such rights by the Commission would constitute an unlawful delegation of the Commission’s authority.

Therefore, for the reasons set forth above, TiVo submits that the MPAA Parties’ request for a formal *independent* role in revocation, renewal, and “Change Management” is unnecessary, unreasonable, and should be rejected by the Commission. As is evident

²² Also, as noted *infra*, TiVo has an independent interest in maintaining the strong security of its system, including the content protected by its system.

from TiVo's Certification, TiVo's technology satisfies the Commission's standards and gives effect to the broadcast flag.

C. A Grant of Third-Party Beneficiary Rights to Content Owners Is Beyond the Commission's Scope of Authority and Would Constitute an Unlawful Delegation of the Commission's Authority

The MPAA Parties ask the Commission to force TiVo to sign an undefined "Content Participant Agreement," with unspecified content owners, giving content owners private rights with respect to the sensitive issues of revocation, renewal, and technology changes, which are clearly the subject of the Commission's Rule. The MPAA Parties ask the Commission to require TiVo to change its private license agreements to grant content owners third-party beneficiary rights "allowing remedies against TiVo or any third-party device manufacturers it licenses TiVoGuard to if the ... compliance and robustness rules are not followed."²³ The MPAA Parties request for the authority to enforce the Commission's Rule in the courts, and their characterization of this right as that of a "third-party beneficiary" to a contract, is merely an effort to cloak an action that exceeds the Commission's authority under statute. As demonstrated below, this proposed delegation of enforcement authority in the nature of government-mandated third-party beneficiary rights is unlawful, unnecessary, and contrary to the goals of the Commission's proceeding.

This delegation of enforcement power to a private party would be unlawful under the circumstances here, and indeed, unprecedented. It is a well-established principle that, absent a Congressional authorization to the contrary, it is unlawful for a federal

²³ Opposition at 9.

administrative agency to delegate its authority to private parties.²⁴ Such delegations are suspect in that they involve private interests that may not be aligned with the national interests that government agencies are charged to protect.²⁵ As the Court of Appeals stated in *U.S. Telecom Ass’n v. F.C.C.*, “while federal agency officials may subdelegate their decision-making authority to subordinates absent evidence of contrary congressional intent, they *may not* subdelegate to outside entities – private or sovereign – absent affirmative evidence of authority to do so.”²⁶ The Court reasoned that

When a statute delegates authority to a federal officer or agency, subdelegation to a subordinate federal officer or agency is presumptively permissible absent affirmative evidence of a contrary congressional intent . . . But the cases recognize an important distinction between subdelegation to a subordinate and subdelegation to an outside party. The presumption that subdelegations are valid absent a showing of contrary congressional intent applies only to the former. There is no such presumption covering subdelegations to outside parties. **Indeed, if anything, the case law strongly suggests that subdelegations to outside parties are assumed to be improper absent an affirmative showing of congressional authorization.**²⁷

²⁴ See, e.g., *Carter v. Carter Coal Co.*, 56 S. Ct. 855 (1936); *U.S. Telecom Ass’n v. F.C.C.*, 359 F.3d 554 (D.C. Cir. 2004); *Shook v. District of Columbia Financial Responsibility and Management Assistance Authority*, 132 F.3d 775 (D.C. Cir. 1998); *National Ass’n of Regulatory Utility Com’rs v. F.C.C.*, 737 F.2d 1095 (D.C. Cir. 1984).

²⁵ See, e.g., *National Ass’n of Regulatory Utility Com’rs*, 737 F.2d at 1143-1144 (stating that, had the FCC delegated its authority over surcharges to local exchanges, “and had the Congress so intended it to act, that would amount to a ‘legislative delegation in its most obnoxious form; for it is not even delegation to an official or an official body, presumptively disinterested, but to private persons whose interests may be and often are adverse to the interests of others in the same business.’”) (quoting *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936)); *Pistachio Group of Assoc. of Food Industries, Inc. v. U.S.*, 671 F. Supp. 31, 34-35 (Court of International Trade 1987) (stating that “[d]elegations of administrative authority are suspect when they are made to private parties, particularly to entities whose objectivity may be questioned on grounds of conflict of interest.”).

²⁶ 359 F.3d 554, 566 (D.C. Cir. 2004) (emphasis added) (holding that the FCC could not delegate to state utility commissions its statutory duty to determine which telephone network elements incumbent local exchange carriers were required to unbundle and make available to competitive local exchange carriers).

²⁷ See *id.* at 565 (emphasis added).

The Court elaborated on the distinction between delegations to subordinates and delegations to outside parties by stating

This distinction is entirely sensible. When an agency delegates authority to its subordinate, responsibility--and thus accountability--clearly remain with the federal agency. **But when an agency delegates power to outside parties, lines of accountability may blur, undermining an important democratic check on government decision-making . . . Also, delegation to outside entities increases the risk that these parties will not share the agency's "national vision and perspective," and thus may pursue goals inconsistent with those of the agency and the underlying statutory scheme. In short, subdelegation to outside entities aggravates the risk of policy drift inherent in any principal-agent relationship.**²⁸

The “policy drift” of which the Court speaks is unquestionably a risk under the MPAA Parties’ proposal. A grant of third-party beneficiary rights to content owners as the MPAA Parties request would amount to a shift in policy *away* from establishing a content protection scheme that balances the rights of consumers, technology providers, and content owners alike, and *toward* a scheme in which content owners alone determine the scope of such rights. There is nothing to prevent a content owner from using these private rights to achieve other, wholly-unrelated business objectives. Were the Commission to turn its authority over to DTV content owners, there would be no restraint on the demands that could be made. This is exactly the sort of “aggravated risk” that the Court in *U.S. Telecom* found unacceptable.²⁹

The MPAA Parties do not cite, and TiVo is unaware of, any “affirmative showing”³⁰ of Congressional authorization for the FCC to delegate its enforcement authority to content owners as the MPAA Parties’ demand. Indeed, some parties to the

²⁸ See *id.* at 565-566 (citing *Nat'l Park and Conservation Ass'n v. Stanton*, 54 F.Supp. 2d 7, 20 (D.D.C. 1999)).

²⁹ See *U.S. Telecom* at 565-566.

³⁰ See *id.* at 565.

Broadcast Protection proceeding have challenged the Commission's authority to promulgate the Rule itself under ancillary powers.³¹ It would be a stretch to also construe the Commission's ancillary authority as giving the Commission the Congressional authorization necessary for it to lawfully delegate its enforcement authority to a private party, through third-party beneficiary rights or otherwise. The Rule does not require delegation of this expansive authority to a third party, or the imposition of third-party beneficiary rights, nor can they be reasonably inferred from the Rule. These are issues that, if they are to be considered at all, should be the subject of a rulemaking. In fact, the MPAA Parties did not propose that content owners be granted these rights in either the Commission's rulemaking proceeding or on reconsideration.³²

Moreover, assuming *arguendo* that such a delegation of authority by the Commission *were* lawful, it should be rejected because such delegation would be unnecessary and absolutely contrary to the goals of this proceeding. As noted above, TiVo is willing to adhere to the Commission's Compliance and Robustness Requirements when manufacturing downstream devices and to require its licensees to do the same. If TiVo fails to enforce these requirements as rigorously as the MPAA Parties would like, the Parties are free to avail themselves of the remedy they requested when they asked the Commission to exercise its jurisdiction in this area – they may file a complaint with the

³¹ See *Report and Order* at ¶¶ 27-29.

³² It appears instead that this issue is being raised at this particular stage to side-track the interim approval process – a process that the Commission already has determined is important. This request has nothing to do with the ability, undisputed by the MPAA Parties, of TiVoGuard to give effect to the broadcast flag. In the initial Broadcast Protection Rulemaking, the only mention of third-party beneficiary rights was in Section X.2(c) of the MPAA's proposed rules. That proposed section related to written commitments by Downstream Product manufacturers to adhere to the compliance and robustness requirements, such as TiVo has agreed herein to provide for it and its licensees. Joint Comments of MPAA *et al.*, in MB Docket No. 02-230, Attachment B at 6 (filed Dec. 6, 2002). Ironically, the MPAA's proposed rules specifically barred the Commission from interfering with private contractual rights. The proposed rules stated that “[t]o the extent that the filing of a written commitment pursuant to this Section X.2(c) creates rights between parties that may be enforced through private contractual remedies or third-party beneficiary rights, enforcement by the Commission will not abrogate those rights and remedies.” *Id.* at 7.

Commission.³³ Also, as noted below in Section III(B), nothing in the Rule bars content owners from exercising their existing rights under the Copyright Act. Yet, in addition to their rights as copyright owners and their right to complain pursuant to regulatory scheme imposed by the Commission, the MPAA Parties are seeking yet a third avenue of enforcement against TiVo and other technology providers.

If the Commission were to grant the MPAA Parties the additional rights they request, TiVoGuard licensees would be subjected to enforcement actions not only from TiVo and the Commission, but from countless numbers of unrelated third parties. It is one thing for the MPAA Parties to demand that TiVo's licensees comply with the Rule and subject themselves to the fair, impartial, and transparent FCC enforcement process; it is quite another to demand that these licensees submit themselves to the mercies of content owner litigation in a variety of state and federal courts. Such litigation will only result in a multitude of inconsistent results among individual courts and the loss of a national standard under the Commission's Rule. In addition, the Commission likely will find itself the final arbiter of such disputes in any event, as some courts, under the doctrine of primary jurisdiction, may well ask the Commission to interpret its own rules. If the primary jurisdiction doctrine is invoked, a court may either retain its ability to make a final ruling on the matter or dismiss the case without prejudice and allow only administrative review. In such cases, the Commission essentially will be deciding liability issues for, and effectively enforcing its own policy decisions in, the federal courts.

³³ Rule at §73.9008(e).

Therefore, TiVo believes that a delegation of enforcement authority in the nature of government-mandated third party beneficiary rights is unlawful, unnecessary, and contrary to the goals of the Commission's proceeding.

D. The TiVoGuard Technology Does Not Place Any Obligation on Content Owners, Broadcasters or Others

The MPAA Parties also request in their Opposition that TiVo clarify that the MPAA Parties are not under any obligation to TiVo as a result of the technology deployed to protect their content.³⁴ In the interest of clarity, and to assuage the concerns of the MPAA Parties, TiVo hereby represents to the Commission that broadcasters, content providers, and others who do not take a license to the TiVoGuard technology but who only mark or broadcast content with a broadcast flag that invokes or "triggers" TiVoGuard are not subject to any obligations to TiVo. Furthermore, TiVo represents to the Commission that consumers are not under any obligation to TiVo for merely transmitting or receiving content marked with the broadcast flag signal.

E. The MPAA Fails to Raise any Objections to the Ability of TiVoGuard to Give Effect to the Broadcast Flag and, Therefore, the Commission Should Approve TiVo's Certification as to Standalone Devices

The MPAA Parties do not take issue with the security of TiVo® DVRs and their ability to give effect to the broadcast flag. In addition, the Parties' concerns regarding scope of redistribution are moot as regards standalone devices because only a PC can permit a user to have access to content outside of TiVo's affinity-based secure viewing groups. Therefore, TiVo's responses to the objections raised by the MPAA Parties, as set forth in this Section II, should permit the Commission to readily approve TiVo's Certification with respect to TiVoGuard for TiVo DVRs.

³⁴ Opposition at 10.

III. TiVo's Proposed Procedures and Technology for "TiVoToGo" Give Effect to the Broadcast Flag and Should Be Approved by the Commission

TiVo's implementation of TiVoGuard in a PC environment ("TiVoToGo") satisfies the Compliance and Robustness Requirements set forth in the Commission's Rule and gives effect to the broadcast flag. In addition, the "local environment" concerns³⁵ that the MPAA Parties expressed with respect to TiVoToGo delve into matters that are outside the scope of this proceeding. Therefore, TiVo's "TiVoToGo" PC implementation should be approved by the Commission.

A. TiVo's PC Implementation Is Secure and Satisfies the Compliance and Robustness Requirements of the Rule

TiVoToGo satisfies the Compliance and Robustness Requirements of the Commission's Rule, and in doing so provides more than the "speed bump" level of protection contemplated by the Commission and the MPAA Parties.³⁶ As TiVo explained in its Certification,³⁷ TiVoToGo allows a consumer to copy recorded content between a TiVo DVR and one or more computers equipped with a hardware plug-in dongle that is registered on the same customer account as the DVR. When a registered dongle is plugged into a computer, a consumer can use that computer to view the transferred content. Because the dongle can only be plugged in to a single computer, only one computer at a time can view transferred content. Moreover, as explained in Attachment A, TiVoToGo uses a proprietary combination of hardware and software to maintain content security and protect against its indiscriminate redistribution.

³⁵ Opposition at 6.

³⁶ In its *Report and Order*, the Commission acknowledged that the goal of the Broadcast Flag content protection system is to "creat[e] a 'speed bump' mechanism to prevent indiscriminate redistribution of broadcast content . . .," and also stated that the MPAA, as an advocate of the ATSC flag system, itself characterized the system as providing a "speed bump" level of protection. *See Report and Order* at ¶¶ 14 (citing MPAA Comments at 12) and 19.

³⁷ *See* TiVo Certification at 6.

The TiVoGuard security system, then, when implemented in a PC environment, effectively inhibits the indiscriminate redistribution of content and, by including a hardware component, provides a level of security that surpasses current industry standards and, in TiVo's belief, any of the PC-based technologies submitted for certification under these proceedings. In short, TiVoToGo gives effect to the broadcast flag. Accordingly, if the Commission were to reject TiVo's Certification with respect to its PC implementation on the ground that it does not provide a speed bump to indiscriminate redistribution of content, it would be tantamount to excluding all PC technologies submitted for certification under these proceedings from the DTV transition.

B. The Distance Limitation Proposed by the MPAA Parties Is Outside the Scope of the Interim Rules and the Commission's Determinations in this Proceeding

Finally, the MPAA Parties question the adequacy of TiVo's "secure viewing group" affinity-based limitation on the redistribution of consumer content, and demand a distance-based limitation on the movement of DTV content.³⁸ The Parties assert that TiVo must limit the proximity of redistribution by "affirmatively and reasonably constrain[ing] unauthorized redistribution from extending beyond a Covered Demodulator Product's local environment – i.e., the set of compliant, authorized devices *within a tightly defined physical space around that product.*"³⁹ This proposed distance or "physical space" limitation is not supported by the Commission's Report and Order or Rule or by any theory supporting the Commission's jurisdiction in this area.

Under the Rule, the guideline for approving or disapproving a proposed technology is simply whether the technology is "appropriate for use in Covered

³⁸ Opposition at 4-6.

³⁹ Opposition at 6 (emphasis added).

Demodulator Products to give effect to the Broadcast Flag.”⁴⁰ Moreover, in establishing the broadcast flag redistribution control system, the Commission repeatedly stated that the goal of the system is to “prevent the *indiscriminate* redistribution of [DTV] content over the Internet or through similar means.”⁴¹ TiVo’s “secure viewing group” feature imposes an affinity-based limitation that is light-years removed from indiscriminate redistribution.

The MPAA Parties’ assertion that a distance-based limitation is the only way to effectively control redistribution of content is not supported by the Final Order or the Rule and is factually incorrect with respect to TiVo’s Certification. As explained in the Certification, TiVo’s “secure viewing group” feature allows content to be exchanged (i) only between devices registered on the same customer account,⁴² and then (ii) only among a maximum of 10 such devices.⁴³ Moreover, each device can be in only one secure viewing group. These restrictions on the number and nature of the TiVo devices that can be placed in a secure viewing group effectively restrict TiVoGuard’s scope of redistribution of digital content, and prevent the indiscriminate distribution the Commission’s proceeding is designed to curtail. As the Commission correctly stated in its Report and Order, the goal of a redistribution control system for DTV should not “foreclose use of the Internet to send digital broadcast content where it can be adequately

⁴⁰ See Rule at §73.9008(a).

⁴¹ See, e.g., *Report and Order* at ¶10 (emphasis added).

⁴² Establishing a TiVo® service customer account requires more than an anonymous registration. A subscriber must register with a valid credit card. TiVo’s possession of customers’ credit card information is yet another reason that security of the TiVoGuard system is of utmost importance to TiVo – TiVo’s failure to protect such sensitive information would undermine customer confidence and place TiVo’s business interests at risk. In addition, a security breach resulting in disclosure of certain TiVo customer information would be required to be publicly disclosed under California law. California Civil Code §1798.82.

⁴³ As noted in TiVo’s Certification, in exceptional circumstances, TiVo may create a secure viewing group that includes up to 20 devices. TiVo Certification at 25.

protected from indiscriminate redistribution.”⁴⁴ TiVo submits that, under these principles, the TiVoGuard system should be approved by the Commission for use in PCs as well as stand-alone DVRs.

TiVo further submits that the MPAA Parties’ objections to TiVo’s “secure viewing group” limitation and the Parties’ demands for a distance-based or “proximity” limitation on the movement of DTV content implicate matters that are outside the scope of this proceeding. In fact, in its Report and Order, the Commission specifically stated:

Our Further Notice of Proposed Rulemaking also seeks comment on the usefulness of defining a personal digital network environment (“PDNE”) within which consumers could freely redistribute digital broadcast television content. **We do not, however, believe that it is necessary at this time to define the precise boundaries of a PDNE in order to initiate a redistribution control scheme for digital broadcast television. Our immediate concern is to adopt and begin implementation of a content protection scheme that will prevent the unfettered dissemination of digital broadcast content through means such as the Internet.**⁴⁵

Moreover, in demanding a distance-limitation standard at this stage, when the Commission has stated that such a standard is not necessary to implement the broadcast flag, the MPAA Parties fail to present any compelling reasons for their demand. The only support that can be found for the “proximity” limits that the MPAA Parties espouse is in the MPAA Parties’ and the Professional and Collegiate Sports Parties’⁴⁶ pleadings in this proceeding – every other commenter has either ignored the call for distance-based limitations or opposed it.⁴⁷ The MPAA Parties conclusively assert that TiVoGuard’s

⁴⁴ See *Report and Order* at ¶10.

⁴⁵ *Report and Order* at ¶10 (emphasis added).

⁴⁶ The Professional and Collegiate Sports Parties include the Office of the Commissioner of Baseball, the National Basketball Association, the National Hockey League, the National Football League, the Women’s National Basketball Association, the National Collegiate Athletic Association, the PGA TOUR, Inc., and the Ladies Professional Golf Association.

⁴⁷ See *In the Matter of Digital Broadcast Content Protection*, MB Docket No. 02-230, FCC 03-273. The following parties opposed the personal digital network environment (PDNE)/local environment standard

affinity-based limitations “raise too many difficult technological, privacy, and legal questions that are not appropriately addressed in this proceeding.”⁴⁸ The MPAA Parties offer no support for, or further elucidation of that statement, and TiVo is at a loss to identify the difficult questions to which the Parties refer. TiVo carefully and in detail explained how its TiVoGuard technology strictly limits content redistribution. TiVo also explained that TiVo rigorously protects user privacy and consumer confidence by protecting the privacy of information that is sent and received by TiVo devices. This information includes anonymous data relating to how customers use their DVRs, as well as information that could be used to identify TiVo customers. As noted in our Certification, TiVo uses the very same security system to protect that sensitive information as it does to protect content.⁴⁹

The MPAA Parties also seem to suggest that the Commission should be a steward of the MPAA Parties’ copyrights, an area that is outside the Commission’s delegated authority. Rather than focusing on indiscriminate redistribution of content, the MPAA Parties appear to be asking the Commission to enter into the business of making sure that “content owners’ rights are not trampled”⁵⁰ The Copyright Office and the courts are the bodies with primary jurisdiction to interpret and enforce the Copyright Act to ensure

proposed by the MPAA Parties: Reply Comments of Aereal, Inc., et. al. at p.4 (filed Mar. 15, 2004); Reply Comments of CE Industry at p.4 (filed Mar. 15, 2004); Reply Comments of Consumer Federation of America at p.1, 7-8, (filed Mar. 15, 2004); Reply Comments of Digital Transmission Licensing Administrator, LLC at p.2-3 (filed Mar. 15, 2004); Reply Comments of Philips Electronics N.A. Corp. at p.25-28 (filed Mar. 15, 2004); Reply Comments of Public Knowledge and Consumers Union at p.6-8 (filed Mar. 15, 2004). The following parties did not address the PDNE/local environment issue: Reply Comments of The American Antitrust Institute (filed Mar. 15, 2004); Reply Comments of The Center for Democracy & Technology (filed Mar. 15, 2004); Reply Comments of The Electronic Frontier Foundation (filed Mar. 15, 2004); Reply Comments of The European Union (filed Mar. 15, 2004); Reply Comments of The Home Recording Rights Coalition (filed Mar. 15, 2004); Reply Comments of Microsoft Corp., *et al.* (filed Mar. 10, 2004); Reply Comments of Silicone Image, Inc. (filed Mar. 15, 2004); Reply Comments of Thomson (filed Mar. 15, 2004).

⁴⁸ Opposition at 4.

⁴⁹ TiVo Certification at 9-10.

⁵⁰ Opposition at 5.

that content owners' rights are not trampled. Protection of all of the rights granted to copyright holders is not what the MPAA Parties requested when they asked that the Commission regulate in this area, and is not what the Commission proposed to accomplish with this proceeding.⁵¹ In fact, in its Report and Order, the Commission specifically stated:

In light of our decision to adopt a redistribution control scheme and to avoid any confusion, we wish to reemphasize that our action herein no way limits or prevents consumers from making copies of digital broadcast television content. **Furthermore, the scope of our decision does not reach existing copyright law.** The creation of a redistribution control regime establishes a technical protection measure that broadcasters may use to protect content. **However, the underlying rights and remedies available to copyright holders remain unchanged. In the same manner this decision is not intended to alter the defenses and penalties applicable in cases of copyright infringement, circumvention, or other applicable laws.**⁵²

The MPAA Parties fail to explain precisely what difficult copyright issues are raised by TiVoGuard, other than to flatly state that electronic transfer of content between user devices is different, and more dangerous, than physical transfer as the MPAA Parties understand it.⁵³ If the MPAA Parties perceive a threat to their business model, they have failed to clearly articulate it, and, in any event, the Commission's proceeding is not designed exclusively to protect the content owners' business model. As Commission

⁵¹ See *Report and Order* at ¶9

⁵² See *id* (emphasis added).

⁵³ TiVo acknowledges that "physical" versus "electronic" is certainly an issue with respect to indiscriminate redistribution. Nevertheless, one merely needs to visit 125th Street in New York City, or the subways of Madrid, where pirate DVDs of current release movies are on sale by street vendors to see that indiscriminate physical redistribution is a real and present danger today, whereas, as the Commission recognized, electronic indiscriminate redistribution is a threat only in the future. As to the limited redistribution a user may engage in, physical redistribution is far more flexible – although it takes slightly more effort – than electronic redistribution. It hardly seems worth the Commission's attention, then, to distinguish between burning a DVD of a TV show and carrying it with you on vacation, and plugging your registered TiVo device into a high speed connection and viewing the local news recorded on your living room TiVo DVR. The significant difference is that a physical copy can be transported to any device in the world and replayed (and, if a digitized analog copy, transferred to any recording device) while the TiVo transfer is limited to a maximum of nine other machines registered to the same user.

stated, the goal of the Broadcast Protection Rule, and the justification for regulatory intrusion in product design, is the promotion of the DTV transition.⁵⁴ It is difficult to imagine how permitting an infinitesimal segment of the device population (no more than ten devices registered by one owner) to transfer recorded DTV programming to his or her own device would inhibit the DTV transition. By enabling a family to time- and space-shift the viewing of a program from their home to their car to their vacation house so that they do not miss local programming while they are away from their house, TiVo's system will promote both the DTV transition *and* localism. Moreover, this functionality is available for NTSC programming, and denying this functionality to TiVoGuard's strictly limited "secure viewing group" would therefore make DTV less capable than analog transmissions, thereby delaying the DTV transition.

The MPAA Parties, in making this "proximity" objection, have failed to articulate a business justification cognizable by the Commission, nor could they given that protection of their business model is not the purpose of this proceeding. Moreover, consideration of this issue is beyond the scope of the Commission's proceeding. The MPAA Parties' objection on these grounds therefore should be disregarded in the Commission's consideration of TiVo's Certification.

IV. Conclusion

TiVo's "TiVoGuard" system gives effect to the broadcast flag. Therefore, as the concerns expressed by the MPAA Parties' in their Opposition are unfounded, TiVo respectfully requests that the Commission approve TiVo's Certification with respect to both DVR and PC implementations of the TiVoGuard system. In the event that the Commission decides not to approve any PC-based technologies submitted for

⁵⁴ See *Report and Order* at ¶¶ 29, 30.

certification in this interim process and therefore does not approve TiVoToGo, TiVo requests that the Commission approve TiVo's Certification with respect to use of the TiVoGuard technology in standalone devices.

Respectfully submitted,

TIVO INC.

/s/ James M. Burger

James M. Burger

Briana E. Thibeau

Dow, Lohnes & Albertson, PLLC

1200 New Hampshire Avenue, N.W.

Suite 800

Washington, D.C. 20036

(202) 776-2300

Its Attorneys

Matthew Zinn
General Counsel
Max P. Ochoa
Corporate Counsel

TiVo Inc.
2160 Gold Street
Alviso, CA 95002-2160

April 16, 2004

Attachment A

TiVoToGo Personal Computer Supplement

TiVoToGo uses a proprietary combination of hardware and software to authenticate and decrypt protected media for immediate and direct viewing by a user. No single component of TiVoToGo can decrypt, authenticate or in any other way access the protected media -- the proprietary software and hardware must both be present for media to be authenticated and decrypted.

At no time is unencrypted media stored or sent across a user-accessible bus (as defined in §73.9000(r) of the Rule). The unencrypted media travels in a direct path from the in-memory TiVoToGo Media Player to the user's screen via a protected bus. The encrypted media and decryption information from the TiVoToGo dongle are brought into memory, the media is authenticated and decrypted, then sent directly to the display via the AGP bus.

I. Components of TiVoToGo

There are four components used in playing TiVoGuard protected media on a personal computer:

- A. A personal computer that includes the following hardware
 - o Mass storage: hard drive, rewritable DVD in data format, etc.
 - o Protected bus display adapter: AGP or equivalent
 - o Connection method for TiVoToGo Dongle, currently a USB port
- B. An authorized TiVoToGo Dongle
- C. The TiVoToGo Media Player
- D. Media that has been protected with TiVoGuard

II. Personal Computer with Appropriate Hardware

A personal computer with a specific set of hardware capabilities is needed to play TiVoGuard protected media. As software and hardware capabilities change over time, TiVoGuard will be restricted to only function on personal computers that meet these specific hardware capabilities.

A. Mass Storage

Mass storage is required to store the protected content. This can be a hard drive, rewritable DVD drive in data format, flash memory, static ram, or any other media capable of storing the protected files. The mass storage is not required to have any sort of protected bus -- the media protected by TiVoGuard is only written, stored and read in a protected form.

B. Protected Bus Display Adapter

A protected bus display adapter is a display adapter that does not allow any outside access to media being sent to a display. The most common and most popular protected bus display adapter uses the AGP standard (see <http://www.intel.com/technology/agp>). In this document we will refer to "AGP adapters" and the "AGP bus" to describe the protected bus display adapter. TiVo will only support TiVoGuard on future display adapter standards that use a protected bus equal to or better than the AGP bus.

C. Connection Method for the TiVoToGo Dongle

A USB port is currently used to attach the TiVoToGo Dongle. Future implementations could use ports or buses similar to USB if they meet the TiVoGuard requirements.

III. TiVoGuard Protected Media

TiVoGuard protects media by encrypting it at two layers. Media is divided into some number of clips, each of these is encrypted with a clip encryption key, or a "clip key." The clip keys are then encrypted with a master key, or a "lead key." The lead key is then encrypted for a specific device -- either a TiVo DVR or a TiVoToGo Dongle -- using that device's public key. Each device has its own public key, no public key is associated with more than a single device. *See* TiVo Certification at 22-24 for a detailed description of the encryption process.

IV. TiVoToGo Media Player

The TiVoToGo Media Player is a software application that is able to authorize and decrypt TiVoGuard protected content and display it directly over an AGP bus. The TiVoToGo Media Player performs specific tasks to ensure that only authorized media is sent to the protected AGP bus for display.

The tasks performed include:

- A. Verify that the TiVoGuard protection on the protected media is intact, valid and was generated by a TiVoGuard compliant system
- B. Contact the TiVo Service to retrieve the current list of invalid/deactivated TiVoToGo Dongles and TiVo DVRs
- C. Determine if an authorized TiVoToGo Dongle is present and functioning
- D. Obtain a list of devices from which this particular TiVoToGo Dongle is authorized to accept and play TiVoGuard protected media

V. TiVoToGo Dongle

The TiVoToGo Dongle is a proprietary USB device that contains several important cryptographic features:

- A. A CPU capable of performing encryption and decryption using the El Gamal algorithm
- B. An El Gamal private key that
 - 1. Is randomly generated on the dongle and never transmitted outside the dongle
 - 2. cannot be read or extracted from the dongle
 - 3. cannot be changed, overwritten or deleted
- C. A unique identification number that is permanently assigned to the dongle

When a TiVoToGo Dongle is initialized at the factory, the Dongle generates its own private and public keys then writes these to a special section of its reserved memory. Immediately after these keys are written, the on-chip hardware that performed this write to reserved memory is destroyed. It is therefore physically impossible to write any new information into an initialized TiVoToGo Dongle's reserved memory. Should this memory become corrupt or fail, the TiVoToGo Dongle is no longer valid and will not function.

The area of memory where the private key is stored cannot be directly read by any means, including by TiVo or during manufacture. The crypto chip in the dongle uses the private key by loading encrypted data into an area of memory and issuing a "decrypt data" command that executes the decryption commands. Because the private key cannot be read from the dongle, there is no way a specific dongle can be spoofed or emulated by software hardware.

Immediately after a TiVoToGo Dongle is initialized, its public key and identification number are stored in a TiVo database. This information is used to manage TiVo customer accounts and authorize devices to participate in TiVo sharing groups.

The TiVoToGo Dongle is used to decrypt a media encryption key ("lead key") using the following steps:

- A. The TiVoToGo Media Viewer application ("the software") determines that a lead key needs to be decrypted
- B. The software verifies that a valid TiVoToGo dongle is present
- C. The software gives the encrypted lead key to the TiVoToGo Dongle
- D. The software sends the "decrypt this encrypted lead key" instruction to the dongle
- E. The crypto chip on the TiVoToGo Dongle decrypts the encrypted lead key using the private key stored on the dongle. **Important:** The private key is never sent outside the dongle or provided to any other hardware or software component by the crypto chip
- F. The TiVoToGo Dongle sends the decrypted lead key to the software

The use of this process guarantees that a TiVoToGo Dongle:

- cannot be spoofed or emulated by a software or hardware emulator
 - there is no way for anyone (even TiVo) to know the private key for any TiVoToGo Dongle
- cannot be reprogrammed to emulate a different TiVoToGo Dongle for
 - there is no way for anyone (even TiVo) to know the private key for any TiVoToGo Dongle
 - the private key on a TiVoToGo Dongle cannot be changed

VI. How TiVoGuard Protected Media is Viewed by a User

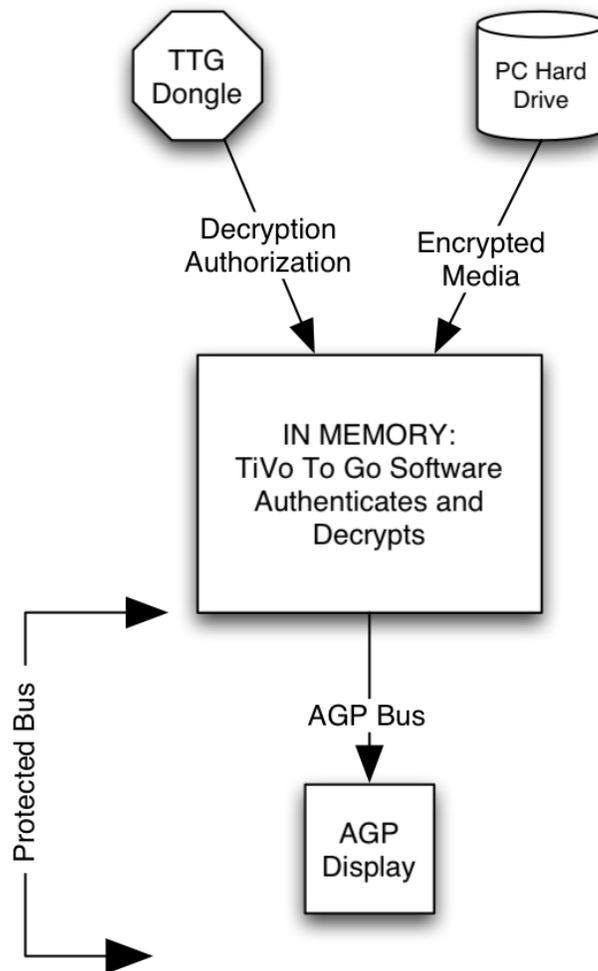
This description of how TiVoGuard Protected media is viewed by a user references the following items:

- PC: a Personal Computer meeting the TiVoGuard requirements for playback of TiVoGuard Protected content
- TiVoToGo Dongle: A TiVoToGo Dongle authorized by TiVo for use
- TiVo Media Player: A software application that implements the TiVoGuard authentication and decryption process and sends the unprotected media directly to the AGP protected bus. This could also be a third-party software application that uses licensed TiVoGuard technology to perform the same operations

Steps performed to display TiVoGuard protected media:

- A. User Decides to Play TiVoGuard Encrypted Media
 1. User attaches the TiVoToGo Dongle to their PC
 2. User launches the TiVo Media Player application and requests that media protected with TiVoGuard be displayed
- B. TiVo Media Player Authenticates the Request
 1. TiVo Media Player examines the media to determine if it is protected with TiVoGuard, and if so, what TiVoToGo Dongle is required to play this media
 2. TiVo Media Player determines if the correct dongle is inserted in the PC
- C. TiVo Media Player Authenticates the Protected Media
 1. TiVo Media Player extracts the encrypted lead key from the protected media
 2. TiVo Media Player sends the encrypted lead key followed by the "decrypt data" command to the TiVoToGo Dongle
 3. TiVoToGo Dongle decrypts the lead key using its internal private key

4. TiVoToGo Dongle sends the decrypted lead key back to the TiVo Media Player
- D. TiVo Media Player Displays the Protected Media
1. TiVo Media Player uses the decrypted lead key to decrypt a clip key
 2. TiVo Media Player uses the decrypted clip key to decrypt a clip of TiVoGuard protected media
 3. TiVo Media Player sends the decrypted media to the AGP protected display bus
 4. AGP protected display bus sends a video signal to the user's monitor



VII. How Media is Protected from Unauthorized Distribution

TiVoGuard protected media is immune to a variety of attack methods.

A. Hardware Attacks

1. **Change the Private Key on a Dongle:** When a TiVoToGo Dongle is initialized, the private and public keys are written to reserved memory on the TiVoToGo Dongle. Immediately after, the on-chip hardware that allowed the information to be written is destroyed. It is therefore physically impossible to write any new information into an initialized TiVoToGo Dongle's reserved memory. Should this memory become corrupt or fail, the TiVoToGo Dongle is no longer valid.
2. **Change the Identification Number on a Dongle:** The identification number on a TiVoToGo Dongle is set during the manufacturing process. It is conceivable that an attacker might be able to change the identification number on a TiVoToGo Dongle in their possession to that of a different TiVoToGo Dongle, or a non-existent TiVoToGo Dongle. However, the attacker would not be able to change the private key on the dongle. While the TiVoToGo Dongle would identify itself as a different TiVoToGo Dongle, it would not be able to decrypt any information encrypted for that different TiVoToGo Dongle because it does not have the other TiVoToGo Dongle's private key.
3. **Third Party Dongles:** TiVo is the only manufacturer of TiVoToGo Dongles, and TiVo's databases only contain records for authorized TiVoToGo Dongles. Should a third party decide to manufacture "clone" dongles, TiVo would not allow customers to register these devices or in any way use them with their existing, authorized TiVo DVRs or TiVoToGo Dongles.

B. Software Attacks

1. **Intercept the Unprotected Video Stream:** The unprotected video stream only exists within on the protected bus, the protected bus adapter, and between the adapter and the monitor used to display video. It is impossible for an ordinary user using generally-available tools to intercept the unprotected stream. See §73.9007 of the Rule.
2. **Emulate a TiVoToGo Dongle in Software:** To emulate a TiVoToGo dongle, an attacker would have to have both a valid TiVoToGo identification number and the corresponding TiVoToGo private key. A given private key only exists in one TiVoToGo dongle and cannot be extracted, recovered or reverse engineered from that TiVoToGo dongle.