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

In the Matter of	)	
	)	
Digital Broadcast Copy Protection	)	MB Docket No. 02-230
	)	

COMMENTS OF TIVO INC.

TiVo Inc. ("TiVo") submits these comments in response to the Federal Communications Commission's (the "FCC's" or "Commission's") Notice of Proposed Rulemaking in the captioned matter.[1] TiVo offers a personalized television service that allows television viewers to take advantage of the incredible convenience of digital technology to customize their viewing experience using advanced searching and storing mechanisms. The TiVo service operates on a secure digital video recorder ("DVR") platform which digitally records television programming onto a hard-disk, enabling the viewer, among other things, to watch its desired programming on a time-shifted basis. The TiVo DVR platform is designed to allow consumers to flexibly use copyrighted content in the home environment while restricting content from exiting the home environment in violation of copyright laws. The DVR hardware component that enables the TiVo service is sold either as an integrated component of a set-top box or as a stand-alone device which works with any multichannel video distribution system.[2]

---

[1] *In the Matter of Digital Broadcast Copy Protection*, MB Docket No. 02-230, Notice of Proposed Rulemaking, FCC 02-231, rel. Aug. 9, 2002 ("NPR").

[2] For more information on TiVo see www.tivo.com.

I. INTRODUCTION

TiVo firmly believes in protecting copyrighted content from unauthorized redistribution outside of the home environment. While the bounds of fair use are difficult to define with precision, TiVo agrees with the Commission that, without adequate protection, digital media is susceptible to piracy because an unlimited number of perfect copies of programming content can be reproduced and redistributed in violation of copyright laws. Consequently, TiVo is highly focused on content security. On the other hand, consumers have a legitimate expectation that they may make limited "fair" use of copyrighted content. The doctrine of fair use is an important element of the policy tradeoff between the exclusive right of copyright owners to control and exploit their creations for a period of time and the public's right to make legitimate use of such creations.

I. DISCUSSION

A. Need For A Regulatory Copy Protection Regime.

While TiVo recognizes the need to protect digital media from unauthorized redistribution, TiVo is not convinced that the consumer marketplace needs the federal government to mandate a copy protection scheme to encourage content providers to permit high quality programming to be broadcast digitally. It is in everyone's interest for media companies to broadcast their content. The issue is to what extent will consumers be permitted to utilize the convenience of digital technology to view that content. Media

companies have been reluctant to permit certain programming to be broadcast digitally because they have not yet reached agreement with technology companies on appropriate business models for such content. It is beyond doubt that the content will be broadcast digitally when the business models are developed.[3] Indeed, there is no guarantee that, if the FCC adopts any particular regulatory regime, content providers will make their "high quality" content available to consumers before appropriate agreements have been entered into between media companies and technology companies.

As described below, TiVo has voluntarily designed its system architecture to protect copyrighted content from unauthorized redistribution outside of the home environment. TiVo does not per se oppose a copy protection regime but is very wary about regulatory creep: the tendency of regulations to expand in scope over time.[4] A regulatory copy protection regime must be (i) narrowly tailored to solve the "problem" of unauthorized redistribution of copyrighted content captured from unencrypted digital television broadcasts; (ii) does not infringe upon settled fair use practice; and (iii) does not eliminate the ability of the market to evolve new fair uses. TiVo is concerned, however, that certain media companies' desires go far beyond protecting copyrighted

---

[3] *See, e.g.,* www.movielink.com where media companies are securely distributing full-length movies to consumers over the Internet. *See also,* Reuters, "Universal Music Unveils Download Plan," *News.Com,* Nov. 19, 2002, http://news.com/2100-1023-966500.html (discussing Universal's plan to sell downloadable songs in response to peer-to-peer services); Strauss, "Online Fans Start to Pay the Piper," *New York Times*, Sept. 25, 2002 at B1 (discussing the progress of the recording industry in offering consumers online subscription services.)

[4] The Broadcast Protection Discussion Group ("BPDG") process itself highlights this concern. The group was formed to discuss the establishment of a means to prevent the unauthorized redistribution of feature films over the Internet. Without any discussion or debate, the scope of the BPDG was expanded at the end of the process to encompass all unauthorized redistribution. Fortunately, in contrast, the Commission's processes ensure that its rules are not subject to change without a clearly defined process providing for notice and comment by interested parties and adequate notice before any change becomes effective.

content from unauthorized redistribution. United States copyright law is designed to strike a balance between an author's rights to control and exploit his work and the public's rights to use that work to promote the free flow of ideas, information and commerce.[5] In this framework, judges are given the responsibility to determine a consumer's fair use rights based on a balance of factors.[6] Sensing a cultural shift, certain media companies are pushing legislation in Congress that seeks to dramatically upset this balance. These companies have adopted a legislative strategy that seeks to scale back settled fair use practices and exert control as to whether, when and how consumers may use copyrighted content. In other words, their goal appears to be "copy control" rather than "copy protection."[7]

B. **The Broadcast Flag**

TiVo does not believe that use of the Redistribution Control Descriptor, as set forth in ATSC Standard A/65A (the "Broadcast Flag") to mark digital broadcast programming would be very effective in protecting copyrighted content from unauthorized redistribution. The Broadcast Flag is inherently weaker security than that

---

[5] *See, e.g., Sony Corp. v. Universal City Studios, Inc.,* 464 U.S. 417, 429 (1984); *Campbell v. Acuff-Rose Music, Inc.,* 510 U.S. 569, 575 (1994).

[6] These factors include (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used; and (4) the effect of the use upon the potential market for or value of the copyrighted work. 17 U.S.C. Section 107 (2002). When confronted with technological change, the Copyright Act must be construed to preserve "the cause of promoting broad public availability of literature, music, and the other arts…." *Twentieth Century Music Corp.,* 422 U.S. 151, 156 (1975).

[7] *See, e.g.,*Weinstein, "Mr Hollywood Lives in Washington," www.wired.com Sept. 30, 2002 (discussing Hollywood's plans to detrimentally reshape and restrict consumer rights with respect to digital technology); Clark and Vaida, "Digital Divide," www.national journal.com Sept. 6, 2002 (discussing the MPAA's legislative agenda). The Digital Millennium Copyright Act ("DMCA") is a case in point. Enacted as the behest of Hollywood, the DMCA has endangered the rights and expectations of legitimate consumers to make fair use of encrypted copyrighted works. *See, e.g., Universal City Studios, Inc. v. Reimerdes,* 111 F. Supp. 2d 294, 321-24 (S.D.N.Y. 2000).

used in smart cards, and smart card security has proven to be quite easy to defeat. More robust security can be achieved by systems employing centralized security, such as the TiVo security system described below.

The TiVo security system is a “trusted authority” architecture using public key/private key encryption and a hardware-based secure microcontroller used for identification and authentication. It enables the secure transfer of digital content among devices in the home. Each device is registered with TiVo so TiVo can authorize which devices are authorized to transfer digital content. Encrypted digital certificates are sent from TiVo to each authorized device in the household. TiVo sends each authorized device the appropriate Public Keys for the other authorized devices and is “signed” by TiVo.

Only authorized devices can request transfers. When device B requests a transfer from device A, device A and B do a secure "key exchange" based on each others' public keys. They then use these “session keys” to in turn encrypt the content keys, which themselves are unique to the device A and change several times within each piece of content. This ensures that the content can be opened only by device B. The digital certificates expire after a set period of time so TiVo can maintain control over which devices are authorized to transfer digital content.

This platform enables a much different type of copy protection than what has been proposed by the media companies: that Congress regulate every consumer electronics product to dictate how consumers can use copyrighted content. The TiVo security system enables consumers to copy any content they receive in their homes and use it in multiple ways within the home environment. At the same time, the TiVo

security system restricts the redistribution of digital copies outside of the home. This platform is more protective of content yet much less damaging to innovation and fair use.

The TiVo platform was developed without regulatory mandate. Rather, it was born of necessity. TiVo believes that partnerships between media companies and technology companies are the best way to benefit all parties, particularly the consumer. For this reason, TiVo believes that appropriate copy protection technologies have and will continue to develop naturally as the digital television transition progresses. Nevertheless, should the Commission conclude that a Broadcast Flag or other copy protection requirement is appropriate, the Commission must ensure that it is narrowly tailored and does not harm established and evolving fair uses copyrighted content. The key is implementation. A Broadcast Flag must not allow content companies to encode content in such a way that imposes restraints on content beyond those reasonably necessary to prevent the unauthorized redistribution outside of the home or home networked environment. Importantly, the instructions contained in the Broadcast Flag should apply at the digital output of a consumer electronic device, not at the input. For example:

- If you have a Device or multiple networked Devices in your home, and a program is marked Copy Once, you should be able to copy the program onto your Device – or copy the program from one Device to another authenticated networked Device in your home – as long as the program can be copied only once upon leaving the secure home network environment, such as a single DVD-R copy.

- If you have a Device or multiple networked Devices in your home, and a program is marked Copy Never, you should be able to copy the program onto your Device – or copy the program from one Device to another authenticated networked Device in your home – as long as the program can not be copied upon leaving the secure home network environment.

- A "one-way" Device, such as a video version of Apple's Ipod mp3 player, where a copy can be made to the Device but a copy cannot be made from the Device, should not have to recognize the Broadcast Flag since it does not have a digital output.

The examples above show how the Broadcast Flag, or other copy protection mechanism, can be implemented without significantly limiting fair uses rights of consumers with respect to digital content.[8] Conversely, were the instructions contained in the Broadcast Flag applied at the digital input of a consumer electronic device, fair use rights could be severely curtailed. Legitimate uses like time-shifting of content could be prohibited at the request of a programmer. Such limitations would serve no legitimate copy protection purpose. Rather, they would exert undue control of how consumers consume lawfully acquired content.[9]

C. Specific Copy Protection Technologies Should Not Be Required.

If a Broadcast Flag or other copy protection regime is adopted, the Commission should not require the use of any particular technology. Rather, companies should be free to choose and/or develop technologies that meet general objective criteria. It is

---

[8] Notably, this paradigm seems fairly consistent with the recent comments of News Corp's Peter Chernin: "[W]e have no objection to anyone making copies of televised content, whether aired on free or pay TV, whether analog or digital, whether recorded on a PVR, a VCR, through TiVo, or with the help of any other device geared to the viewer's convenience. The trumpeters of the Big Bully Theory may also be startled to learn that we have absolutely no problem with viewers shifting our content from their television to their PC, from their living room to their bedroom and to their bathroom and back again as many times and ways as they'd like. What we are looking to accomplish is a balance between the viewer's right to take advantage of the unprecedented convenience of digital technology and the content creator's right not to be digitally looted…. We have zero objection to anyone's ability to duplicate, to record, to play back and to save any copyable content whatsoever." Peter Chernin, *The Problem With Stealing,* Comdex, Fall 2002 Keynote, Nov. 19, 2002.

[9] *See* Brad King, "TiVo Might Rue Arrival of DTV," August 7, 2002, www.wired.com/news/business/0,1367,54358,00.html ("The next generation of digital video recorders will be equipped for DTV, and there will be more shows and options for the viewer than ever; but if Hollywood gets its way, consumers won't enjoy the features that TiVo or ReplayTV offer now.")

absolutely critical that media companies not be able to block new technologies or devices.[10] Companies should be free to innovate within the bounds of these objective criteria.[11] TiVo suggests that the following criteria would be appropriate:[12]

> All Devices that receive and/or record digital television signals shall employ digital output copy protection designed to prevent unauthorized redistribution outside of the home or home network environment. Such digital output copy protection shall meet the following criteria with respect to content containing a Broadcast Flag:
>
> - Require a company to construct a physical device of sufficient complexity to be beyond the capability of an ordinary consumer to either defeat such technology, to avoid the application of such technology, or acquire the keys to an encryption system (which shall be a minimum of 56 bits in length).
>
> - Preserve the Broadcast Flag with the content or keep other information identifying the content as protected with the content during digital output and transmission over a digital interface, provided that if content is identified as protected by such other information, it shall be treated as protected if the Broadcast Flag is not preserved; and
>
> - Authenticate the device receiving content via the digital output copy protection technology using a cryptographic authentication method or hardware handshaking method that prevents promiscuous snooping on the interface in order to confirm that the receiving product complies with the rules for digital outputs.

As long as a company's devices functionally comply with these objective principles, the company should not require any further authorization or approval to manufacture such

---

[10] Media companies' veto power over new technologies or devices is a fundamental problem with the BPDG's recommendations. While the media companies ultimately backed off their insistence on an absolute veto right, the BPDG settled on an arbitration process whereby technology companies must overcome MPAA objections before a neutral arbitrator before new technologies will be added to the list of approved technologies for use by a DTV technology vendor. Such a long, expensive, and uncertain arbitration process will effectively dissuade all but the largest technology companies from engaging in this process and will stymie innovation.

[11] It is highly doubtful that consumers would have videocassette recorders or DVD recorders if technology companies were required to obtain acceptance of new technologies from the media companies.

[12] These criteria are based on Philips Proposal to the BPDG ("X.12 Criteria for Technologies To Be Admitted to Table A."

devices. Independent entities should be able to "certify" that a particular digital output copy protection technology meets these objective criteria. Disputes as to whether any particular technology satisfies these principles could be resolved by the Commission under existing procedures.

III. CONCLUSION

While digital media needs to be protected from massive unauthorized redistribution, TiVo is not convinced federal intervention is warranted. Copy protection techniques far more effective than a Broadcast flag have and will continue to develop naturally as the digital television transition progresses. Nevertheless, should the Commission feel compelled to impose that consumer electronics devices recognize a Broadcast Flag or other copy protection mechanism, the Commission must ensure that this requirement is implemented in a way that does not harm established and evolving fair uses copyrighted content. The Commission should not adopt a copy protection regime that unduly restricts the incredible consumer convenience, flexibility, and innovation engendered by digital technology.

Respectfully submitted,

TIVO INC.

By: _____

Matthew P. Zinn
Vice President, General Counsel &
Chief Privacy Officer
2160 Gold Street
Alviso, California 95002
(408) 519-9311

December 6, 2002