



October 3, 2002

Marlene H. Dortch, Esquire
Secretary
Federal Communications Commission
445 12th Street, NW
Washington, DC 20554

**Re: Notification of *Ex Parte* Communication
MB Docket No. 02-230**

Dear Ms. Dortch:

This is to advise you, in accordance with Section 1.1206 of the FCC's rules, that James Barton, Howard Look and I ("TiVo") had a telephone call yesterday afternoon with the following Commission staff members: Rick Chessen, William Johnson, Thomas Horan, Steve Broeckaert, Alison Greenwald, and Amy Nathan.

The discussion involved the Notice of Proposed Rulemaking, released on August 9, 2002 in the above-referenced docket and many of the questions noted therein. Among the specific items under discussion were TiVo's concerns about certification and robustness requirements associated with a broadcast flag approach proposed by the Motion Picture Association of America ("MPAA") and the 5C companies (the "Proposed Regulation").¹ Specifically, TiVo is concerned with any scheme in which the major studios and the 5C companies would effectively determine "authorized technologies" under the Table A criteria contained in the appendix to the Proposed Regulation.² The delegation to private parties with huge financial interests in the outcome of the critical right to designate the technology used by DTV device manufacturers simply would not be in the public interest. The MPAA has little

¹ Comments of the Motion Picture Association of America, in MB Docket No. 02-230 (filed Dec. 6, 2002) ("MPAA Comments").

² TiVo shares the concerns of Philips and others in this regard and supports the certification approaches suggested by Philips. See Letter from Lawrence R. Sidman to Marlele H. Dortch, Esq., Secretary, Federal Communications Commission, filed in MB Docket No. 02-230, on September 23, 2003 on behalf of Philips Electronics North America Corporation ("Philips Letter").

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

Tel 408.519.9100 • Fax 408.519.5333 • www.tivo.com

incentive to approve new technologies and the 5C companies have the incentive to encourage other companies to license their proprietary technology under their terms and conditions and discourage the development of competing technologies.³ The practical effect of delegating the right to determine the technology used by DTV device manufacturers to a group of financially interested parties will be to stymie advances in technology - like TiVo digital video recorders and services - that benefit consumers by providing them with some measure of control over their television viewing while protecting copyrighted content from unauthorized redistribution outside of the home environment.

TiVo believes that securing content is absolutely critical, and does not oppose a broadcast flag in principle. However, the key is in how the flag is implemented. TiVo urged the Commission, if it decides to act in the area, to at least establish functional specifications for permitted content protection systems to get on the "Table A" list and allow manufacturers to certify that their products comply with such specifications.

With respect to robustness, TiVo explained that there are two domains of security contemplated in the Proposed Regulation: "within receiver" domain, called demodulator security, and the "between devices" domain, or so-called "Table A" security.

With respect to demodulator security, much of the Proposed Regulation imagines requiring "bank vault" levels of security, including special tools for accessing the internals of the demodulator, obfuscation of source code and security techniques, and immunity to commonly available software tools, such as de-compilers. This approach might seem to provide enhanced security for operation of the demodulator and protection of unscrambled content, but in reality it fails to do so for the following reasons:

- (1) Special tools can be manufactured as needed, and are easily sold over the Internet or other channels;
- (2) Obfuscation invariably fails as a security strategy, as is continually demonstrated, for example, De-CSS for DVD. A motivated individual or group will spend whatever resources and time is needed to discover the operation of the demodulator. Once discovered, this information may be easily disseminated over the Internet, and all value of the obfuscation is then lost;
- (3) Software tools for exploring and attacking a system are only going to become more sophisticated and powerful over time. Indeed, just the advent of a new Pentium processor can provide sufficient horsepower to make previously innocuous tools useful for attacking the security of a receiver.

³ The practical consequences of permitting private licensing terms associated with "authorized technology" to harm innovation and competition is amply demonstrated in the Philips Letter at p. 4 and Appendix C.

- (4) Demodulator internals and secrets may be disseminated by accidental or malicious exposure, invalidating the security provisions taken in the demodulator design.

Further, there are significant costs for the manufacturer of the device. For instance, debugging and validating that a design operates correctly becomes very difficult. As a result, the actual product unnecessarily will be more expensive for the consumer. Any robustness rules need to be reasonable and technically feasible. They should enable manufacturer to develop products that thwart "ordinary users" using "commonly available tools" in their efforts to defeat content protections rather than determined hackers.

TiVo has taken an alternative approach. As described in Attachment A hereto, TiVo provides a service to its subscribers that have many of the properties of a secure content broadcasting service. Rather than using a "bank vault" method, the TiVo approach relies on insuring that the receiver never executes untrusted software. Secure content delivery is accomplished by following the "chain of trust": A secure, embedded ROM is responsible for loading an operating system kernel, and checking that the kernel has not been tampered with, using the public signing key for the TiVo Service. If the kernel is valid, it is given control of the system, at which point it performs the same validation on all operational software and files. If this step succeeds, it is known that all software in the receiver is valid and trusted, and normal operation begins. Otherwise, the receiver fails to start.

The TiVo approach provides security at least as good or better than the "bank vault" approach, while granting other advantages such as lower cost to manufacture. In approaching a definition of demodulator robustness for unencrypted content, TiVo therefore urges the Commission to consider a simpler requirement by specifying:

"Covered Demodulator Products shall be manufactured in a manner that provides sufficient mechanisms to assure that unauthorized modifications of operational software are possible only by direct modification of trusted hardware components, such modifications being beyond the capability of the ordinary user, using commonly available tools, and likely to damage the device."

This definition encompasses the "TiVo approach" as well as the "bank vault" approach, should a manufacturer wish to pursue that path.

Given the complexities and critical nature of the robustness and compliance rules contained in the Proposed Regulation, if the Commission does decide to proceed with adoption of a broadcast flag regime, TiVo supports the IT Coalition's call for the Commission generally to approve the tagging of HDTV broadcasts with a flag as a

Ms. Marlene Dortch
October 3, 2003
Page 4

signaling method, while issuing a further rule making notice seeking comment on the critical and complex issues of robustness and certification rules for technologies authorized for digital broadcast copy protection.⁴ Dictating technology (or delegating the power to do so) is highly unusual for the FCC and any actions in this regard must very, very carefully considered. Robustness and certification rules should not be adopted even as “interim” requirements without additional notice and comment from affected parties. These requirements undoubtedly will have profound effects on technology companies and consumers and there is absolutely no reason for the FCC to rush to judgment on these critical issues.⁵

As required by section 1.1206 of the Commission’s Rules, 47 C.F.R. Section 1206, one copy of this letter is being filed electronically in the above-referenced docket. Please direct any questions concerning this matter to the undersigned.

Respectfully submitted,

Matthew P. Zinn

Matthew P. Zinn
Vice President, General Counsel & Chief Privacy Officer

cc: Rick Chessen
William Johnson
Thomas Horan
Steve Broeckaert
Alison Greenwald
Amy Nathan

⁴ See Letter from James M. Burger to Marlene H. Dortch, Esq., Secretary, Federal Communications Commission, filed in MB Docket No. 02-230 (filed Oct. 2, 2003) on behalf of the Business Software Alliance and the Computer Systems Policy Project (collectively the “IT Coalition”).

⁵ *Id.* at p. 2 (the problem of video downloading is “three or four years away” (quoting MPAA President and CEO Jack Valenti)).