

Rhonda M. Bolton
202.429.6495
rbolton@steptoelaw.com

June 25, 2003

Via ELECTRONIC FILING

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

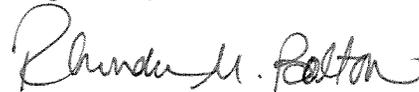
Re: *Ex Parte* Presentation – In the Matter of Digital Broadcast Copy Protection,
MB Docket No. 02-230

Dear Ms. Dortch:

In its comments and reply comments in the above-captioned proceeding, Veridian Corporation (“Veridian”) has expressed its view that “source encryption” is a far superior digital copy protection method to the broadcast flag technology that is currently the subject of the above-referenced Commission inquiry concerning digital broadcast copy protection. Veridian is far from alone in holding that view: a number of the comments and reply comments submitted by other participants in the rulemaking have pointed to the inferiority of broadcast flag technology as a means of digital copy protection. For the Commission’s convenience, Veridian has assembled relevant excerpts from those comments in the attached matrix. As Veridian also has argued, these comments are part of a record that cannot support the universal prescription of the broadcast flag, contrary to its proponents’ request.

One copy of this *Ex Parte* Notice is being filed electronically with the Commission as permitted by Section 1.1206 (b)(1) of the Commission’s Rules.

Respectfully submitted,



Rhonda M. Bolton
Counsel for Veridian Corporation

Enclosure

Ms. Marlene H. Dortch
June 25, 2003
Page 2

cc: Chairman Powell
Commissioner Abernathy
Commissioner Adelstein
Commissioner Copps
Commissioner Martin
Mr. W. Kenneth Ferree
Mr. John Wong

Summary of Comments and Reply Comments Acknowledging Inferiority of Broadcast Flag

FCC Notice of Proposed Rulemaking Proceeding on Digital Television Copy Protection
MB Docket No. 02-230

Commenter Name	Commenter Interest	Statements Acknowledging Inferiority of Broadcast Flag
Digital Transmission Licensing Administrator LLC ("5C")	Copy protection technology vendor	-- DTLA licenses 5C digital transmission content protection, and helped develop the broadcast flag proposal. DTLA acknowledges that "[f]rom a technical perspective, protection is most effective when applied at the source, such as distribution of content in an encrypted form." DTLA assumes (without explanation) that DTV broadcasters will not be using encryption, and therefore, the "next most effective means" to protect content is applying protection at the point of demodulation. (DTLA Comments, p. 7)
Motorola	Copy protection technology vendor; consumer electronics manufacturer	-- the broadcast flag, as currently defined without source encryption, is ineffective; any valuable content must be encrypted at the source; source encryption is overwhelmingly accepted as mandatory among the professional security technology community, and is used in other contexts such as cable and satellite TV, DVD, cable modem, Internet browser cable telephony and digital cellular networks; digital television ("DTV") should be no different. (Motorola Comments, p. ii; pp. 4-5)
Philips Electronics North America Corp.	Consumer electronics manufacturer	<p>-- the record in this proceeding dispels the myth that the broadcast flag enjoys consensus support (Philips Reply Comments, p. 6); in fact, many parties object to the MPAA's proposal. (<i>Id.</i> at 3-6)</p> <p>-- the flag will not even achieve its core purpose of effectively preventing unauthorized redistribution of content over the Internet. (<i>Id.</i> at 3)</p>

Commenter Name	Commenter Interest	Statements Acknowledging Inferiority of Broadcast Flag
		<p>-- the broadcast flag proposal's "hands-off" approach to unprotected analog outputs is what makes the system unacceptably deficient in preventing unauthorized redistribution of content. (<i>Id.</i> at 12, 14)</p> <p>-- any DTV content protection regime implemented by the Commission should "[b]e established and implemented through <i>open processes</i> in which the public has a full opportunity to comment and, if necessary, petition for change, rather than be the exclusive province of private parties with vested interests." (Philips Comments, pp. 15-16 (emphasis in original))</p>
National Music Publishers' Association, <i>et al.</i> ("NMPA")	Content providers	<p>-- NMPA and fellow reply commenters do not object to use of the broadcast flag as an indicator of content subject to protection beginning at the radio signal demodulator, but "are interested in whether the subsequent protection for content identified by the flag is adequate in light of the fact that the digital data accompanying the flag is completely unencrypted and in the clear." (Joint NMPA Reply Comments, pp. 6-7)</p> <p>-- detailed technical requirements should not be mandated by the FCC, nor should the Commission pick one or more specific compliant solutions; it might, however, be helpful for the Commission to set "results-oriented standards." The FCC might require that any technology not rely on "shared secrets" (citing the DVD protection scheme as an example of a failed "shared secrets" regime). (<i>Id.</i> at 10-11)</p>
TiVo, Inc.	Personalized TV service provider	<p>-- the broadcast flag is inherently weaker than security systems such as the one used by TiVo, as the latter employs a "trusted authority" architecture using public key/private key encryption and a hardware-based microcontroller used for identification and authentication. (TiVo Comments, pp. 4-6)</p>

Commenter Name	Commenter Interest	Statements Acknowledging Inferiority of Broadcast Flag
Public Knowledge and Consumers Union	Consumer groups	<p>-- transmitting content “in the clear,” as the broadcast flag proposal suggests, “leaves the front door open” to infringement (Public Knowledge & Consumers Union Comments, p. 14)</p> <p>-- the nominal cost of the broadcast flag proposal may be more expensive to society as a whole because such a regime would require that all devices recognize the flag in order to be effective; indeed, it would be more cost-effective to mandate or subsidize satellite dishes for those households that cannot obtain or afford cable or satellite service -- the end-to-end scrambling systems of satellite and cable systems do not have the flaws of “marking”- based copy protection like the broadcast flag. (<i>Id.</i> at 12)</p> <p>-- any content protection scheme requiring the content to be broadcast “in the clear” [such as the broadcast flag] is inherently and conceptually flawed. (Public Knowledge & Consumers Union Reply Comments, p. 4 n.6)</p>
Electronic Frontier Foundation	Civil liberties interest group	<p>-- the broadcast flag is “an absurdly weak form of security technology” because it can be circumvented by noncompliant receivers, legacy devices, and analog outputs (i.e., the analog hole.) (Electronic Frontier Foundation Comments, pp. 7-8)</p> <p>-- the broadcast flag is “more sieve than solution.” Several holes exist, including the: analog hole; legacy receivers hole; software receivers hole; cable hole (represented by unencrypted terrestrial DTV broadcasts or ones encrypted using relatively simple means transmitted on basic cable tier); and the 480p DVI hole (proposal would permit unprotected DVI outputs so long as they limit resolution to no more than 480p, but this provides no protection to broadcasters like Fox that broadcast large portions of their lineup in 480p.) (Electronic Frontier Foundation Reply Comments, pp. 9-13)</p> <p>-- DVDs’ “break one-break everywhere” security system demonstrates the ineffectiveness of a security system like the flag. (<i>Id.</i> at 14)</p>

Commenter Name	Commenter Interest	Statements Acknowledging Inferiority of Broadcast Flag
IT Coalition	Industry group comprised of the Business Software Alliance and Computer Systems Policy Project	<p>-- during the Broadcast Protection Discussion Group (“BPDG”) proceedings, the computer industry “proposed encrypting DTV prior to transmission, . . . based on its extensive experience in protecting digital content.” (IT Coalition Comments, p. 16-17)</p> <p>-- a broadcast flag regulation might be effective today, “but such effectiveness is not likely to last. . . . Protection at the source would be a better solution.” (<i>Id.</i> at 17, n.44)</p> <p>-- “the technology industry would prefer that the FCC signal its agreement that broadcasters may encrypt DTV content at the source.” (<i>Id.</i> at 15); doing so would make industry negotiated solutions similar to that unanimously agreed to by the consumer electronics, movie and computer industries in the case of DVD’s, easier to achieve. (<i>Id.</i> at 18)</p> <p>-- “If the Commission determines that it must oversee management of content protection of material originally provided through DTV broadcasts, it should establish objective, technical, and licensing criteria for content protection but not select a particular compliant solution.” (<i>Id.</i> at 19-20).</p> <p>-- “ a more effective solution . . . [than the broadcast flag] would be for the FCC to state explicitly that broadcasters may encrypt DTV content at the source and endorse that approach as the most effective means to address the threat of piracy.” (IT Coalition Reply Comments, p. 4)</p>