

**Before the
Federal Communications Commission
Washington, DC. 20554**

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

**COMMENTS OF THE
ELECTRONIC PRIVACY INFORMATION CENTER**

December 6, 2002

The Electronic Privacy Information Center ("EPIC") respectfully submits these comments concerning the Federal Communications Commission's ("FCC") Notice of Proposed Rulemaking ("NPRM") discussing digital broadcast copy protection.

EPIC recommends that no broadcast flag mandate be issued by the Commission unless affirmative consumer privacy protections, consistent with established public policy, are incorporated into the mandate and the broadcast flag standard. While EPIC recognizes the legitimate interest of the copyright industry in protecting against the unauthorized redistribution of their content, the broadcast flag standard as currently presented in the Broadcast Protection Discussion Subgroup report ("BPDG report") leaves open the possibility for privacy invasive copy protection devices, and also restrains competition more than is necessary to accomplish the goals of the copyright industry. EPIC recommends further study of potentially privacy-invasive applications of the broadcast flag prior to any FCC mandate. The FCC should also preserve the ability of consumers to consume broadcast content anonymously.

The Electronic Privacy Information Center ("EPIC") respectfully submits these comments in response to the Federal Communications Commission's ("Commission") Notice of Proposed Rule Making ("NPRM") discussing digital broadcast copy protection.¹

EPIC encourages the Commission to conduct further study of potentially privacy-invasive technologies that may utilize the broadcast flag.

I. INTRODUCTION

EPIC is a not-for-profit research center in Washington, DC that seeks to protect privacy, the First Amendment, and constitutional values. EPIC's interest in digital broadcast copy protection lies in the ramifications of the broadcast flag mandate on individual privacy.

Congress has established a federal legal statutory framework to promote the laudable public policy goal of protecting consumer privacy with regards to viewing and title information. For

¹ Notice of Proposed Rulemaking, FCC 02-231, released August 9, 2002.

instance, the Cable Communications Policy Act provides a strong statutory framework for the protection of cable subscribers' personally identifiable information, requiring cable providers to obtain the prior written or electronic consent of the subscriber before collecting or disclosing such information.² The Act also grants subscribers the right to access the data collected about them and to destroy personally identifiable information that is no longer needed to provide the service. Furthermore, the Video Privacy Protection Act prohibits the disclosure of video rental records containing personally identifiable information, except in special circumstances such as pursuant to a federal criminal warrant.³ A broadcast flag-enabled device could collect this protected information. Broadcast flag technology should not serve as an end-run around established public policy, and thus the FCC should not issue any rule until affirmative consumer privacy protections are incorporated into the mandate.

II. THE BROADCAST FLAG WILL BE INEFFECTIVE IN ENCOURAGING DTV BROADCAST.

The Commission has stated that the present lack of digital broadcast copy protection hinders progress of the digital television ("DTV") transition.⁴ Content providers claim to be reluctant to broadcast high quality digital programming due to concerns over the unauthorized copying and redistribution of content. The Commission wishes to advance the DTV transition by implementing a system that will make unauthorized redistribution of protected content more difficult for home viewers.

However, the efficacy of the broadcast flag in facilitating the transition process is dubious. A regulatory copy protection regime is not necessary to expand the current DTV transition. CBS, for instance, recently announced that it will develop programming for DTV.⁵ Other content providers are likely to follow suit, if only to keep up with the competition, thereby eliminating the need for federal imposition of standards for digital content protection.

It is also unclear that the proposed mandate will prevent the unauthorized content redistribution that the copyright industry seeks to control. Given the millions of legacy devices on the market, the presence of general purpose computers, and the weak protection the broadcast flag system provides, the increased incentives for content providers would appear to be quite distant. If the primary concern of the broadcasters is unauthorized redistribution over the Internet, only one unprotected copy needs to be made in order to thwart the copy protection scheme. Papers from a recent conference of computer scientists on Digital Rights Management suggest that the possibility of creating even a moderately effective copy protection system is quite low.⁶

Furthermore, the proposed transmission-side flag mandate may raise barriers to entry, potentially precluding both new consumer electronic manufacturers and smaller broadcasters from the market, as such groups may not be able to afford to implement this technology. The decision of whether to incorporate the flag would be better left to content providers and consumer electronic

²47 U.S.C. § 551.

³18 U.S.C. § 2710.

⁴ Notice of Proposed Rulemaking, FCC 02-231, released August 9, 2002.

⁵See <<http://www.cbs.com/info/hdtv>> for the current CBS HDTV line-up.

⁶<<http://crypto.stanford.edu/DRM2002/prog.html>>

manufacturers on a voluntary basis. If an effective but flexible and non-intrusive technology is available, then it may be adopted without a government mandate.

III. MODIFICATIONS TO THE BROADCAST FLAG STANDARD

The standard discussed by the Broadcast Protection Discussion Group ("BPDG") in its Final Report is ambiguous and unsettled.⁷ The members were not able to reach a consensus on several key issues, including compliance and robustness requirements and the scope of protection to be accorded to DTV content. EPIC suggests that the Commission delay adoption of the standard pending the resolution of these issues.

Furthermore, the Commission should incorporate a quid pro quo rule into any standard it chooses to adopt. If content providers are demanding mandated copy protection as a prerequisite to digital broadcasting, they should be required to initiate DTV broadcasts in return for this regulation. Such a requirement would ensure the achievement of the ultimate goal of the proposed standard—to advance the DTV transition.

Additionally, the Commission should incorporate an avenue for review and/or revocation of the standard after a set number of years. If personally identifiable information is integrated in the technology, the flag should be revoked until a privacy framework is in place. For example, any collection of personally identifiable information from a broadcast flag-enabled device should be strictly "opt-in," and allow the consumer unfettered access to the same content anonymously. If the flag proves inefficient and fails to achieve the goal of expediting the DTV transition, the mandate should expire.

IV. RISKS TO PRIVACY

A. Because the robustness and compliance requirements are not articulated in the BPDG report, the door remains open for privacy-invasive applications of the broadcast flag. A broadcast flag standard should not be adopted until affirmative privacy protections are included in the robustness and compliance requirements.

Copy protection technologies based on the broadcast flag could potentially implicate important privacy interests. Since the BPDG report fails to specify the compliance and robustness requirements for approved devices, it leaves the door open to the incorporation of privacy-invasive technologies into devices which handle DTV content. Absent any affirmative privacy protections in the Commission's mandate or in the compliance and robustness requirements, strong incentives exist to deploy privacy-invasive copy protection techniques as they may be the most effective way to enforce the content industry's interests. The Commission should thus incorporate privacy requirements into the broadcast flag mandate, and furthermore should prohibit the use of the broadcast flag in cases where it would be used to violate personal privacy in a way inconsistent with the established public policy embodied in the Cable Communications Policy Act, the Video Privacy Protection Act, and other federal privacy statutes.

⁷BPDG Final Report at 14-17.

i. Metered Use Applications

One categorical example of a potentially privacy-invasive application of the broadcast flag is the SmartRight copy protection and content management system developed by Micronas and Thomson Multimedia.⁸ According to a company press release, the system "meets commercial requirements for content protection in devices for digital home entertainment networks such as TV sets, Set-Top-Boxes, DVD players, digital video recorders, and PCs," and thus is likely to qualify for incorporation into "approved devices" under the broadcast flag standard. The SmartRight technology provides end-to-end content protection and is targeted towards the redistribution of protected content within the home, an activity that the BPDG report states should be permitted under the broadcast flag standard.

A company representative describes the technology as one which "help[s] content owners create a new business revenue model." SmartRight recognizes an "entitlement control message" such as the broadcast flag and enforces whatever rules are specified in the message. Content owners could use the technology to charge consumers every time their digital content is re-distributed within the home, or viewed multiple times.⁹ Used in this way, the broadcast flag would enable content providers to log the exact viewing habits of the consumer, invading the privacy of the viewing public and establishing an unwarranted level of control on the part of the broadcaster. These collections of data are contrary to the public policy established in the Cable Communications Policy Act and the Video Privacy Protection Act. The FCC should prohibit any application of the broadcast flag which provides a mechanism for individual viewing habits to be reported back to content providers as incompatible with basic privacy rights within the home.

ii. Renewability/Revocation Authority

The broadcast flag also raises privacy concerns when applications include a renewability/revocation system. Given that copy protection systems are inevitably compromised over time, newer digital rights management implementations often include a mechanism for a remote entity to revoke the device's authority to decode protected content, or alternatively require a remote renewal signal in order to continue functioning past a certain time. Consumer electronics devices using the SmartRight system, for example, will be equipped with a removal security module (such as a smart card) that complies with current protection standards and can be upgraded as such standards change.

Should a particular class of devices enforcing broadcast flag protection become compromised, content providers might revoke the ability of those devices to demodulate digital content. Consumers would then be forced to upgrade their system, possibly revealing their personal identity or incurring significant expense in the process. The Commission should prohibit revocation and renewability systems in broadcast flag applications, or at a minimum require any such system to function anonymously.

⁸<<http://www.thomson.net/gb/01/01671.htm>>

⁹Junko Yoshida, Content protection plan targets wireless home networks, EE Times, Jan. 17, 2002.

Furthermore, the BPDG report suggests that "significantly compromised" technologies should be removed from Table A. If technologies are removed from Table A, consumers should remain free to use and service previously purchased devices. The FCC should insure that the content industry is prevented from investigating the use of legitimately purchased devices, even after they are removed from the list of acceptable technologies.

iii. Circumvention Detection

Copy protection systems employ a number of methods to detect circumvention attempts. In some cases, a device may cease to function entirely until the manufacturer or some other third party reenables it. For example, many computer DVD players will not allow the "region" setting to be changed more than a limited number of times, and the user is then required to send the player back to the manufacturer to be reset, revealing their name and address and possibly other personal information. Other circumvention detection methods include actually reporting back over the Internet to the content provider or to the device manufacturer about the attempted breach of security.

The Commission should mandate that any anti-circumvention technologies incorporated into devices that recognize the broadcast flag should not require any remote device renewal or other privacy-invasive system.

B. The professional and broadcast use exception to the compliance and robustness rules also raises privacy concerns.

The BPDG report states that proposals currently under consideration for the compliance and robustness requirements would exempt products specifically intended for professional and broadcast use. Making a specific set of technologies available exclusively to one category of people raises a number of questions which implicate privacy interests: Would an individual seeking to purchase exempt products be required to prove that the device would not be used in other environments? Does the Commission intend to establish penalties for using professional grade equipment in the home environment? Given the rapidly dropping cost of digital media devices, will professional grade devices become accessible to the average consumer, thereby undermining the purposes of the broadcast flag mandate? Over the past decade, devices which were once only affordable to large content creators are now commonplace in homes and schools. Individuals should not have to reveal the intended uses of their purchases, and the professional/consumer technology distinction may erode over time.

C. By imposing a privacy-invasive and limiting technology on the consumer, the broadcast flag mandate may undermine its own stated goal of advancing the transition to DTV.

While the purpose of the Commission's broadcast flag mandate is to provide incentives for content providers to invest in digital broadcasting, the restrictions it would impose on consumers and the potentially privacy-invasive applications of the flag could work against this goal. Consumers generally avoid products that are inconvenient or invasive. A leading example is Digital Audio Tape ("DAT") recorders, which by law are burdened with so many copy protection

features (such as the Serial Copy Management System, which intentionally degrades the quality of DAT copies) that consumers generally have rejected them.¹⁰ No matter how many incentives the FCC establishes for broadcasting companies to provide digital content, the transition will not occur if consumers lose interest in purchasing DTV-related devices.

Over the past decade, consumers have eagerly adopted unencumbered digital media devices such as CD and DVD players and burners, portable MP3 players, digital video cameras, and television receiver cards for computers.¹¹ If these devices become inflexible or privacy-invasive as a result of the broadcast flag mandate, demand for these new technologies could drop. The Commission should consider effects on consumer demand and its impact on the underlying purpose for the broadcast flag. While to some degree this presents a "chicken and egg" problem, it is important to remember that there are two sides to the market equation, and simply satisfying the content industry's requirements may not advance the desired transition.

V. VERTICAL INTEGRATION

By establishing a gateway role for the content industry in adding devices to the Table A approved technologies listed, the broadcast flag mandate establishes unnecessary barriers to entry for new technologies. While any technological mandate on consumer electronic devices technologies is likely to have an anticompetitive effect, the Commission should adopt a standard which minimizes interference with market competition. Any mandated copy protection system should establish a level playing field for all manufacturers, and not favor those companies that are involved in the BPDG.

The anticompetitive nature of the technology approval process could encourage the adoption of more privacy-invasive technologies. Since any new technology would have to win the support of the content industries, manufacturers may focus their efforts on strengthening content protection rather than maximizing consumer privacy or technological flexibility. Privacy interests would be better served by neutral technical specifications for new devices. Devices meeting these specifications should be presumed to comply with a broadcast flag mandate, and any challenges should be arbitrated by the Commission rather than by the content industries.

VI. CONCLUSION

EPIC requests that the Commission conduct further study to examine the efficacy of the flag in protecting digital broadcast content from improper redistribution. It is likely that the proposed standard will be an ineffective means of achieving this goal.

If the flag is indeed adopted, it is of paramount importance to ensure that consumers' privacy interests are protected consistent with established public policy. The Commission should, therefore, incorporate affirmative consumer privacy protections into the proposed broadcast flag standard for digital broadcast copy protection. At a minimum, the flag should not be adopted

¹⁰Charles C. Mann, Taming the Web, Technology Review, Sep. 1, 2001.

¹¹See, e.g., Consumers Will Spark 200% Rise in Recordable DVD Sales in 2003, Business Wire, Nov. 17, 2002.

until clearly delineated compliance and robustness requirements have been set that comport with basic principles of consumer privacy.

Respectfully submitted,

Marc Rotenberg
Executive Director

Chris Hoofnagle
Legislative Counsel

Adam Kessel
IPIOP Clerk

Diana Oo
IPIOP Clerk

Electronic Privacy Information Center
1718 Connecticut Ave NW, Suite 200
Washington, DC 20009