Digimarc Comments for BPDG 5/21 Final Drafts

May 28, 2002

DIGIMARC

Digimarc Corporation
19801 72nd Ave., Suite 100
Tualatin, OR 97062 USA

Digimarc Comments for BPDG 5/21 Final Drafts

1 Executive Summary

Digimarc is encouraged by the time and effort invested by members of the BPDG, representing several industries, to address the problem of unauthorized redistribution of unencrypted digital terrestrial broadcast television and is hopeful that this same level of energy and commitment continues to address the larger issues of protecting multiple forms of digital and analog content.

Digimarc believes that the Broadcast Flag can provide a measure of security for free-to-air broadcast content if adopted on a widespread basis and when it is appropriately used with a number of additional security technologies to protect and manage the content. However, the Broadcast Flag is not technically sufficient as a solution to protect broadcast content from unauthorized distribution. The broadcast flag leaves analog outputs unprotected and these outputs, which are readily available in more than 95% of U.S. homes today and will be available for the foreseeable future, can easily be used to copy and redistribute broadcasts.

As such, we believe that it is appropriate for the report to note that additional methods of signaling the no redistribution state are necessary and that these requirements will be modified at some future time to allow additional methods to secure the broadcasts and analog outputs (a.k.a. the analog hole). We suggest that BPDG or other appropriately chartered group start work to examine these security holes immediately.

1.1 Document Organization

This document has two main parts. The first part, comprised of sections 2 through 6 includes an overview of the current partial solution, remaining problem, and a more comprehensive solution to protect digital terrestrial broadcast television and related content where the analog hole is secured. The second part, comprised of sections 7 and 8, discuss suggested changes for both the draft report and draft requirement documents.

Problem and Complete Solution

2 Broadcast Flag is a Partial Solution

The focus of BPDG, as indicated in its charter, is the prevention of unauthorized redistribution of unencrypted digital terrestrial broadcast content. Conforming devices, upon detecting marked content, are required to protect the digital output of the device. Using the Broadcast Flag to mark the content is a step forward in protecting content but only provides a partial solution since the analog outputs can easily be used to access, copy and redistribute the content (a.k.a. the analog hole).

3 Addressing the Analog Hole

The analog hole has also been discussed inside and outside the BPDG. The analog hole has been defined by Richard Parsons, CEO of AOL Time Warner at the Senate Judiciary Hearing of March 14th, 2002 as:

> "Video content, even when delivered digitally in a protected manner, must be converted to an unprotected analog format to be viewed on the millions of analog television sets in consumer homes. Once content is "in the clear" in analog form, it can be converted back into digital format which can then be subject to widespread unauthorized copying and redistribution, including over the Internet. This problem applies to all delivery means for audiovisual content, from DVDs to pay per view, to over the air broadcasts."

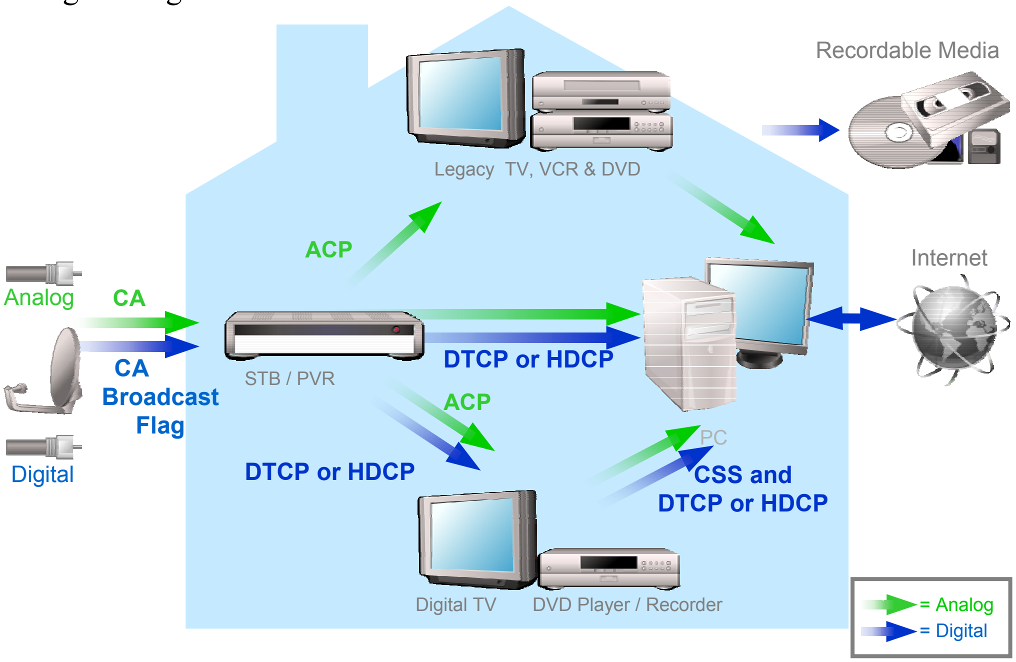
The main problem with the Broadcast Flag is that two analog holes exist:

- Analog outputs of Covered Products (X.3.a.1 and X.4.a.1)
- Analog broadcasts (i.e. NTSC, PAL, SECAM)

These analog holes enable DVD-recorders and PCs to capture analog video, convert it to digital and compress it. We believe that analog video provides reasonable quality for Internet redistribution for the foreseeable future. This is based upon the observation that video redistributed on the Internet is significantly compressed. Thus, recording analog broadcast or the analog output of covered devices will produce similar quality video as recording the digital output of covered devices and recompressing to a similar low bit rate.

An additional open issue includes backwards compatibility during the transition period, defined as the period during which analog broadcasts are converted to digital broadcasts and TVs begin receiving standard (SD) and high (HD) definition digital input. Currently, the vast majority of Digital TVs employ a STB ATSC receiver with analog HD connections to a CRT monitor. In addition, OpenCable STBs provide for analog HD connections to the CRT monitor. These analog HD connections are not currently provided with any form of protection and would not be protected by the Broadcast Flag.

An exemplar system with only the Broadcast Flag is shown below, where unprotected content can easily be copied and sent to the Internet or recordable media from the legacy analog and digital channels.



4 Protecting Digital Broadcast Requires Securing the Analog Hole

The analog hole must be secured to provide an effective solution for protecting digital broadcast content. Technologies have been identified to help secure the analog hole and the digital domain, as noted in the following recent quotes from leaders in the technology, motion picture, and government sectors:

> "Watermarks may provide a means to ensure that protection rules survive as content transitions analog outputs."
>
> Dr. Craig R. Barrett, President and CEO, Intel Corp. Senate Judiciary Hearing, March 14th, 2002.

> "We are developing a plan to plug the "analog hole" that includes harnessing watermarking technology that would prevent such conversions from being used to avoid content protection obligations"
>
> Peter Chernin, President and COO, News Corporation
> Senate Commerce, Science and Transportation Committee
> Hearing, February 28th, 2002.

> "One way to plug the analog hole is through the use of watermarks…. some government action will be needed to require appropriate detection of and response to the watermark."
>
> Richard Parsons, CEO, AOL Time Warner, Inc.,
> Senate Judiciary Hearing, March 14th, 2002

> "The most promising technical solution for this so-called "analog hole" appears to be watermarking copy control technology…"
>
> The Honorable Patrick Leahy, U.S. Senator, Vermont,
> Chairman of Senate Judiciary Committee,
> Senate Judiciary Hearing, March 14th, 2002

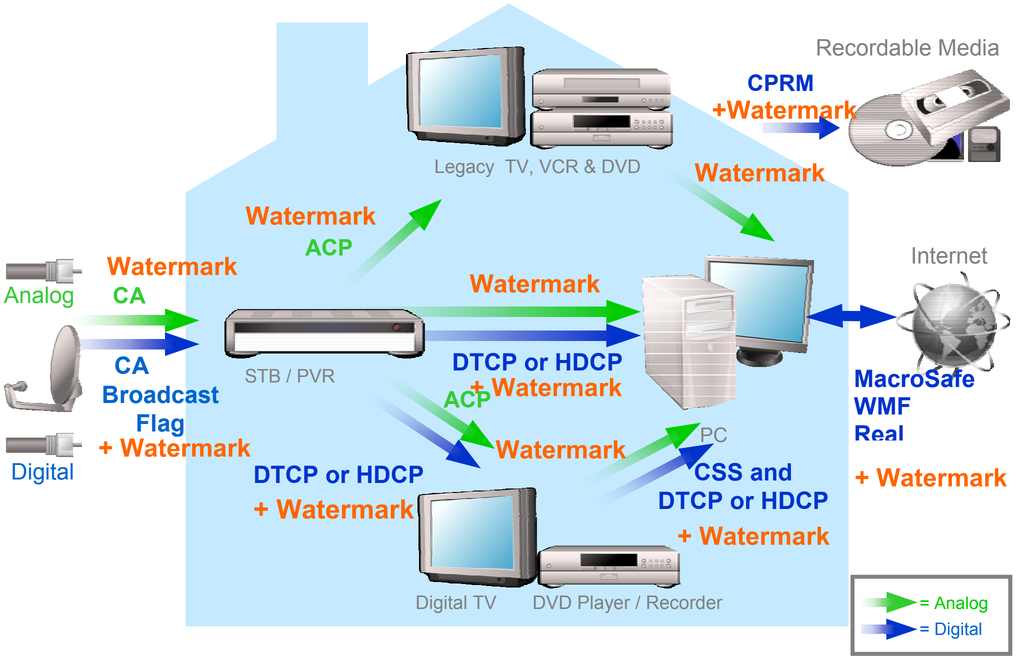
Securing the analog hole with the Broadcast Watermark has been discussed within the BPDG. The Broadcast Watermark was originally identified as an alternative in the November 28th presentation by 5C to the CPTWG, which created the BPDG, and included in the statement of work. It has also been previously discussed in News Corp/Fox's submission of December 20th 2001, Macrovision's response to the Feb 15th draft, Digimarc's response to the interim draft progress report, and referenced in some technology proposals and discussion comments from CE company members of the BPDG.

5 Securing the Analog Hole

To provide an effective solution for protection of broadcast content, the analog and legacy digital domains must be secured (i.e. secure the analog holes). Without a complete solution, pirates will take the path of least resistance to bypass the security provided by the broadcast flag. In other words, they will copy the content from a quality analog output and re-digitize it, rendering the digital protection ineffective.

We believe that in order to comprehensively prevent unencrypted digital television from unauthorized redistribution, the "analog hole" must be secured and that a Broadcast Watermark must be considered for use. In addition to providing protection against the "analog hole", a Broadcast Watermark could provide another layer of security alongside the Broadcast Flag as a signaling technology since it can remain with the content in non-covered devices and connections, and enable the content to be protected when entering a covered device.

An example complete system, where the content is always controlled on the Internet or within recordable media from the addition of a Broadcast Watermark is shown below.



5.1 *Broadcast Watermark and Broadcast Flag Synergistic Effects*

In order to truly protect the content and eliminate the redistribution and piracy of broadcast content, it is important to use available technology. This should include not only the Broadcast Flag, but also a Broadcast Watermark. Together these technologies can help protect both digital and analog content, including analog content that has been digitized for redistribution or playback.

The Broadcast Watermark provides three synergistic effects with the Broadcast Flag:

- Protecting the two analog holes
- Backwards compatibility during the transition period
- Additional layer of security that allows re-assertion of rights with covered devices

The Broadcast Watermark robustly protects content for the following analog holes:

- Analog outputs of Covered Products (X.3.a.1 and X.4.a.1)
- Analog broadcasts (i.e. NTSC, PAL, SECAM)

The protection remains with the content all the way to the point that it is susceptible to redistribution to the Internet.

The Broadcast Watermark is backwards compatible during the transition period. This enables protecting analog outputs for legacy DTVs.

The Broadcast Watermark also enables an additional layer of protection on top of the Broadcast Flag and any resulting encryption, for all protected digital outputs. As such, if the Broadcast Flag is removed or the encryption is compromised, the Broadcast

Watermark remains. The Broadcast Watermark can force the reassertion of usage rights when content transitions into a covered device.

5.2 Synergies between Broadcast and DVD consensus Watermark

If the Broadcast Watermark is compliant with the DVD consensus watermark, compliant DVD recorders and PC recorders will not illegally copy broadcast content. This protection can be limited to analog channels, but can easily include digital channels. Given the availability of watermark technology that can be used to address the problem of protecting broadcast content there is no reason not to proceed with the utmost speed in defining and implementing a Broadcast Watermark.

5.3 Alternative Architectures

Just like a Broadcast Flag, a Broadcast Watermark could be used by a variety of implementations that protect content downstream including both the architecture proposed by the 5C and the “flag preserving” architecture proposed by Philips. It is also backwards compatible with legacy equipment, which means that no consumer will be left with unusable legacy equipment.

In these alternative architectures, the Broadcast Flag cannot work in the analog domain since robust out-of-band solutions are not available. The Broadcast Watermark can work in the analog domain as well as the digital domain; thus working synergistically with the Broadcast Flag. In fact, a Broadcast Watermark is beneficial to the Broadcast Flag because, as being part of the content, it is inherently preserved without specialized hardware.

6 Conclusion

In conclusion, in order to prevent unauthorized redistribution of unencrypted digital terrestrial broadcast television, the “analog hole” must be addressed. Since the presence of the “analog hole” essentially renders the protection provided by the Broadcast Flag ineffective, it needs to be addressed in tandem with implementation of the Broadcast Flag. A Broadcast Watermark can protect the analog output of covered devices, is backwards compatible and preserved with existing DTVs and DVD players, and enables an additional layer of protection on top of the Broadcast Flag and resulting encryption. The advantages of a Watermark approach are based upon the fact that the Watermark is part of the content, not an out-of-band channel, and survives conversion between the analog and digital domains as well as digital format conversion.

The Broadcast Watermark can also be standardized to work with compliant DVD and compliant PC recorders, thus protecting current NTSC analog broadcasts. This additional protection is not a focus of BPDG; however, it is implicit if a robust watermarking technology is used.

Technology to address the “analog hole” exists and can be applied to provide the protection necessary to prevent unauthorized redistribution of broadcast content and help ensure consumers can benefit from new content, distributed in new ways, using the new technologies that are becoming increasingly widespread. We encourage the members of the BPDG to consider all of the available technologies to protect digital broadcast content and embrace a comprehensive solution. The work to identify appropriate, comprehensive, solutions for protecting broadcast content could be done under the auspices of the BPDG or another, appropriately chartered, working group. However structured, the work to address the “analog hole” needs to be completed coincident with proposals to adopt or mandate use of the broadcast flag in order to provide the necessary protection of unencrypted digital broadcast television.

Specific Suggested Changes for Draft Reports[1]

7 Draft Final Report Comments

In the "Background" section 1.6, we suggest text to indicate that broadcast watermarking was considered as a necessary component in the original Nov 28th presentation as well as the presentation (ContentProtection.pdf) by Fox from 12/20.

In "The Work of the BPDG" section 2.4, we suggest text to indicate the securing the analog hole must be addressed in order to have a technically sufficient solution to protect the content.

In "The Summary of Conclusions" section 4.1, we suggest text indicating that the "broadcast flag" is a good step towards a complete solution, but not technically sufficient since the analog holes easily enable anyone to access, copy and redistribute content.

In addition, we suggested modifying footnote 7 to indicate the BPDG or another group needs to consider additional technologies, such as a Broadcast Watermark, since additional technology is necessary for a complete solution. Otherwise, we have spent a lot of time providing a partial, easy to circumvent security system.

In the "Summary of Points as to which Consensus was Not Reached," we added section 5.10 to clarify that consensus was not reached on how to address the analog hole or the potential use of additional technologies, such as a Broadcast Watermark, to do so.

8 Draft Final Compliance and Robustness Requirements Comments

In the "X.1 Definitions" section we added a footnote indicating the definition of marked content may be modified if a broadcast watermark is used.

We added a section "X.12 Future Modifications" that anticipates changes to the requirements when the "analog hole" problem is addressed and when broadcast watermarks are used.

[1] We have included language in the draft final report and draft final compliance and robustness requirements, with changes tracked, that corresponds to these suggested changes.