Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Telecommunications Policy 28 (2004) 503–521
TELECOMMUNICATIONS POLICY
www.elsevierbusinessandmanagement.com/telpol

Understanding the broadcast flag: a threat analysis model

Allan Friedman[a,*], Roshan Baliga[b], Deb Dasgupta[b], Anna Dreyer[b]

[a] *John F. Kennedy School of Government, Ph.D. Mailboxes, 79 JFK Street, Cambridge, MA 02138, USA*
[b] *Massachusetts Institute of Technology, USA*

Received 1 April 2004; received in revised form 1 May 2004

Abstract

The broadcast flag is supposed to protect digital broadcast content from unauthorized distribution. This paper critically examines the broadcast flag as a security mechanism in the context of digital content control. A threat model analysis from the computer security field is presented as a framework for evaluating the flag. The model identifies stated and potential goals of the flag's proponents and evaluates how well the flag protects these goals from diverse attacks. The paper finds that the flag does not adequately protect content from Internet redistribution and highlights a new intellectual property paradigm that the broadcast flag does protect.

Keywords: Digital television; Intellectual property; Security; Risk analysis; Internet content

1. Introduction

Digital content protection has grown into a huge issue over the past 10 years. As the ability to make and distribute perfect copies of digital content becomes ubiquitous and cheap, content owners fear the widespread dissemination of their copyrighted materials over the Internet, particularly over peer-to-peer systems that have proven hard to shut down. The advent of digital television (DTV) offers yet another benefit of the digital information age, and also threatens to open other means of digital infringement if users can freely capture and distribute broadcast TV shows and movies. While one of the main drivers behind DTV is the release of Hollywood movies, premium content companies, represented by the Motion Picture Association of America (MPAA), are reluctant to release their content without some sort of protection.

*Corresponding author. Tel.: +1-617-943-2190.
E-mail address: allan_friedman@ksg.harvard.edu (A. Friedman).

0308-5961/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.telpol.2004.05.011

To resolve this issue, content owners met with broadcasters, consumer electronic companies and other interested parties. The resulting proposal was the broadcast flag. This simple digital signal, attached to a digital broadcast signal, would control how the content could be used, to which devices it could be sent and how many times it could be copied. The MPAA claims that this scheme will protect their content and, if it is implemented into the DTV infrastructure, they will freely release their content. Implementation requires the support of a variety of other actors, each of whom claims to support the flag as well. Opponents feel the proposal is ineffective, overly broad and restrictive of the freedoms to which users are accustomed with their media content.

The broadcast flag debate has not been without hyperbole, yet a comprehensive framework for policy analysis has been noticeably absent. This paper proposes an analytic frame within which to examine the veracity and robustness of the MPAA's claims, and the efficacy of the broadcast flag as effective policy. After a summary of the history and goals of the broadcast flag, a threat model analysis adapted from the computer security field is presented. Possible goals of actors under the flag regime are suggested, and the flag is evaluated in terms of how well it defends those goals from attacks. The paper further tests this model by relaxing assumptions and find that the flag does not protect content against unauthorized distribution. After examining the harms introduced by the broadcast flag, the paper concludes that embedding digital rights management in such a widely used system is poor policy.

2. Digital television and the broadcast flag

The broadcast flag was suggested as a consequence of the emergence of DTV. DTV offers many benefits over analog television since it improves picture and sound, and requires less bandwidth for broadcast transmission. The FCC created the Advanced Television Systems Committee (ATSC) in 1995 with a mandate to develop standards for DTV, and broadcasters began implementing the switch to DTV. While maintaining analog broadcasts, digital broadcasts began using additional spectrum granted by the FCC. DTV is considered an improvement over the standard analog transmission that uses the NTSC standards because it can transmit more data more efficiently. This enables a better picture quality, under what is known as high definition television, or HDTV. By late 1998, the 26 TV stations in the country's most populous cities began broadcasting using the DTV system. Full transition to digital format is scheduled to occur by 2006, when every station would be expected to transmit all content digitally under FCC mandate. This deadline appears to be in question now, however, but a speedy transition remains a goal for regulators and broadcasters (Hachman, 2004).

Transition requires consumer buy-in, since the signal demodulators that turn radio waves into images on existing televisions are not compatible with the new signal, but adoption of this new technology has not matched expectations. Over the past few years, consumer adoption of HDTV-compliant sets has been lagging. As of mid-2003, roughly 6 million sets had been sold (Joseph & Miller, 2003), out of over 100 million households with a television (Nielsen Media Research, 2001). Networks attempted to encourage HDTV subscriptions by offering a range of programming in high definition format; however, the lackluster adoption rates gave broadcasters little reason to invest in the more costly HDTV-formatted content. This shortage of visually

appealing content, compounded with the high price tag, gave consumers little reason to invest thousands of dollars for DTV sets (Goroch, 2001).

Some attributed the slow adoption of DTV to the lack of quality, visually appealing content on terrestrial television. Many looked to the MPAA to provide that content on DTV, but the MPAA has claimed that member companies are reluctant to release content without copyright protection enforcement. Owners of premium content fear the widespread, unauthorized distribution of their content on the Internet. Unlike DVDs and cable, which are, respectively, stored and transmitted under encryption, digital broadcasting must be delivered unencrypted. In fact, the FCC currently requires that this terrestrial broadcast television be sent "in the clear" as part of its mandate, so that any commercially available set can demodulate the broadcast signal. The MPAA fears delivering high-quality, unencrypted content digitally because viewers could digitally record shows and later make them available as downloadable files on the Internet for widespread, unauthorized distribution.

In an effort to address this problem, the Copy Protection Technical Working Group (CPTWG), composed of representatives from entertainment, information technology and consumer electronics industries, formed the Broadcast Protection Discussion Group (BPDG) to develop guidelines for copy protection of content provided over digital terrestrial television. The goals of the group include developing a technical specification for the broadcast flag and recommending the implementation of that specification.

A conceptualization and partial specification of the broadcast flag was issued in the Final Report of the Co-Chairs of the BPDG in 2002. It describes a system in which the broadcast signal is marked with a flag indicating the copy permissions of that content. The demodulating device that interprets the digital signal will only pass the digitally accessible content to devices that securely and reliably indicate that they will honor these copy protections. The specifications for these devices and the standards compliant with the demands of the flag are described in what has become known as "Table A". This is a list of technologies in the BPDG Final Report that meet the approval of the Discussion Group for adequately protecting content, including encrypted buses[1] and digital media storage that preserves the flag. Most of the technologies on the list to date have been developed by the 5C consortium, which comprises Sony, Hitachi, Intel, Matsushita and Toshiba. There has been some controversy surrounding what standards are employed in assessing qualifications for entrance onto Table A. Philips, Thomson, and Zenith (2002), for example, have objected to an unfair bias in favor of 5C technologies. If the technologies are selected, all will be subject to the final standards of broadcast flag compliance.

The flag is explicitly designed to limit which devices to which content can be sent, and those devices can be designed to treat content in a specific fashion. However, it is not completely clear to what degree this will accomplish the stated goals of the designers. The exact implications of how users will be affected by full implementation are the subject of much legal and ethical debate. An exact prediction is almost impossible given the matters yet to be decided, and is outside the scope

[1] A 'bus' is a data channel that moves information from one part of the computer (typically the memory) to another part (typically a processor of some sort). Data transmitted without encryption can be read by anyone with access to the bus, that is, anyone who has opened up the computer and can read the bus output. Encrypting information over the bus is important for "strong" security.

of this paper. Instead, the paper examines how effective it will be at its stated goals, and speculate what other goals the flag could serve.

3. A threat model framework

How effective will the broadcast flag be at doing what it is supposed to do? While the MPAA clearly states that the broadcast flag is designed only to prevent "unauthorized redistribution of copyrighted content, not prohibit digital copying" (MPAA, 2002), others claim that it is unfriendly to consumers and will push MPAA goals that many believe to be bad policy. This paper presents a threat model analysis to evaluate the efficacy of the broadcast flag.

The broadcast flag is, at its heart, a security mechanism. Although it is simply a component in a digital information stream, it is designed to control access, and ensure that the wrong actors cannot take unauthorized actions. It thus follows that the scheme should be analyzed from a security standpoint, rather than from the standard economic and legal tests. Fortunately, the computer security field has ample experience in analyzing and evaluating a security system.

Security expert Schneier (2003) presents a simple yet very powerful tool to analyze a risk control system called a "threat model analysis". As Schneier presents it, a threat model analysis has five components, directing the practitioner to:

1. identify assets to be protected,
2. identify risks to those assets,
3. assess how well the security mechanism protects the asset from the risk,
4. explore new risks introduced by the security mechanism,
5. assess costs and trade-offs of implementation.

This model does not give its user a clear answer, but rather provides an analytic framework within which to evaluate whether a security mechanism should be implemented.

In this threat analysis, the paper examines the effectiveness of the broadcast flag in accomplishing the stated goals of the MPAA, in addition to other speculated motives. In doing so, it considers all possible threats to the broadcast flag as a security protection against attacks on several goals, and the parties that may accomplish these threats. It concludes that the broadcast flag is not an effective means of preventing digital content distribution over the Internet, but will be successful in promoting other possible, although unstated, goals of the content owners. The paper then assesses several other weaknesses in the broadcast flag approach, and examine the costs and claims of those who oppose the flag.

This threat analysis uses two key hypothetical assumptions. The first assumption is that the Table A components, as part of DTV, are commonplace. Consumers have been induced to switch to DTV, and the analog broadcasts have been discontinued. Almost all homes have replaced their legacy televisions with DTVs. Since the flag is meaningless without compliant devices, this assumption is necessary to analyze the flag in action.

A more important assumption is that *the analog output from all DTV tuners has been restricted*. The analog output of media devices forms a "hole" in digital rights management efforts, since any analog output signal can be re-recorded as a digital signal through an analog input. Various factions of the digital content media have begun to work on this problem; it is hard to imagine a

solution that does not involve more hardware regulation. The justification for this assumption is that if the so-called "analog hole" is not blocked, then the broadcast flag will have no effect in preventing the Internet redistribution of movies, since it is trivial to redigitize an analog video stream. The assumption is revisited below in the discussion of realistic constraints, but for this model it is necessary in order to clearly examine how the flag will protect assets from threats.

4. Assets and threats

For the purposes of threat analysis, three potential assets, or goals of the MPAA in proposing the broadcast flag are examined:

- The actual content being broadcast under the broadcast flag.
- The business model of schedule-driven broadcast television.
- The paradigm of intellectual property.

The first goal requires the elimination or near elimination of illegal distribution of movies on the Internet. The second involves a restriction of personal recordings of movies for time-shifting or library building; the final goal is a move toward the reversal the societal norms allowing copyright infringement and a shift of control of content into the hands of the copyright holder.

Note that the last two goals have not been publicly identified as being goals that the MPAA wishes to accomplish by passing broadcast flag legislation. Rather, they are goals that seem reasonable in light of what the broadcast flag makes possible. The threat model analysis requires that exploration is made of the asset space to the fullest extent to see exactly what the flag will accomplish. Each of these goals and consequent threats are examined below.

4.1. Goal 1: elimination of illegal distribution of movies on the Internet

The MPAA's stated goal of the broadcast flag is to prevent the illegal distribution of movies over the Internet. According to the MPAA, the broadcast flag "signals that the program must be protected from unauthorized redistribution" (MPAA, 2002). The same public statement further clarifies the point to apply to Internet distribution, and clarifies why preventing distribution is an asset: "If unauthorized copies of programs are widely available on the Internet they cannot be sold in ancillary markets and the owners cannot cover the costs of production." MPAA constituents fear a loss of revenue through this unauthorized distribution chain, and may wish to prevent this problem before it escalates.

Currently most consumers do not have the bandwidth to download full-length movies in a reasonable amount of time. For example, a 2-h movie encoded using the DivX codec takes about 10 h to download over a cable modem with standard 100–150 kilobytes, compared to 2 min for the average song encoded in the MP3 format. While illegal copies of movies are not as prevalent as MP3 music files on the Internet, it is possible that future advances in bandwidth will give rise to a movie trading community, perhaps over peer-to-peer networks. Protecting this asset is a reasonable goal, and has been explicitly stated.

For the purposes of this threat model, it is assumed the attack has been successful even if a very small number of people manage to release a movie on the Internet. Compared with personal control, which is discussed below, a single unauthorized copy can undermine a protection scheme using peer-to-peer systems. Decentralized networks, such as Gnutella and Limewire, have proven resistant to attempts to shut them down, either by technical means or through legal action (Smith, 2003). In these peer-to-peer networks, as more users download the file and keep it available for others to download, it becomes easier to find and download by others, spreading exponentially across the network. Therefore, in a peer-to-peer network, if the original source of a file is not stopped prior to sharing of the file, it is impossible to prevent the spread of the file, provided the file is in demand. This paper does not seek to challenge the validity of monetary loss claims, but rather focuses on the Internet distribution itself. Another assumption made is that the MPAA is only concerned with the distribution of HDTV-quality movies. For the purposes of this threat analysis, it will ignore the Internet distribution of movies that are "ripped" from DVDs, rather than broadcast HDTV.

There are many threats to the goal of preventing unauthorized distribution of movies on the Internet. The paper distinguishes between three capable adversaries of meeting the goal of preventing Internet distribution of digital content: average consumers, nefarious infringers, and groups with resources.

4.1.1. Average consumers

The average consumer may wish to distribute movies on the Internet to share them with friends, or simply to share them with anyone. Movies may be distributed in their entirety, or as short clips. The paper defines this group as having enough comfort with technology to find file-sharing software and operate it to upload and download files, but no particular technical competence to evade strong protections without a user-friendly interface.

Since it is assumed that the analog output would be disabled, digitization of content is not an option. Consumers will somehow have to work around the broadcast flag to disseminate movies over the Internet since the broadcast flag is designed explicitly to prevent movies from being moved to computers. The average consumer must thus have the interest, knowledge and resources to use a circumvention device. While the broadcast flag is not currently in use, comparisons can be made with older copy protection methods, such as the Content Scrambling System (CSS) encryption used in DVDs. CSS encryption was broken in 2000, and DVD decryption software is widely available on the Internet (Patrizia, 1999). Evasion of CSS to distribute copies, however, remains somewhat limited. Of traded movies, only a fraction is digitally ripped from DVDs. Many are captured from cinemas or stolen screening tapes. An analysis of ripping versus trading of music files reveals similar conclusions, that only a few peers in a peer-to-peer network generate and share most of the files (Adar & Huberman, 2000). Most users do not transfer content from legitimate to illegitimate sources, but download files others have removed from their original context. This conforms to the content industry's claim that file-swappers are primarily interested in acquiring content for free.[2] Those merely seeking to consume will be stopped from freeing

[2] "The term 'file sharing' is a popular euphemism for copying, which…is stealing." Fritz Attaway, "Copyright Privacy Prevention and the Broadcast Flag" *Testimony to the House Committee on the Judiciary, Subcommittee on Courts, the Internet and Intellectual Property* March 6, 2003.

content from its original media by a fairly low entry barrier; they will instead download and then share the handiwork of others.

It is therefore claimed that the flag imposes too large a technical obstacle for the average consumer, who is only casually interested in distributing files him or herself. The flag is specifically designed to block casual misuse. The average user will not engage in the necessary effort to circumvent a robust implementation of the flag. In this model, the group of ordinary consumers does not pose a serious threat to the broadcast flag's primary goal.

4.1.2. Nefarious infringers

These "nefarious infringers" are a much smaller group than the average consumers. They will have some technical knowledge, and are willing to expend energy in learning how to circumvent copy protection mechanisms. This group may distribute movies on the Internet for monetary compensation, but the more likely reason is that they simply enjoy distributing movies. Monetary compensation is unlikely to be a driving force of nefarious users because of the difficulty in receiving payment for the sale of illegal merchandise without getting caught. For some, an increased reputation for them or their friends in various Internet social networks is incentive enough to undertake extensive efforts to evade copy protections. To extend the prior comparisons, this is the group that converts songs to the MP3 format and compresses decrypted DVD content for Internet distribution.

To distribute HDTV-quality movies on the Internet, this group must circumvent the broadcast flag. While a full discussion of the technical robustness of the broadcast flag is beyond the scope of this paper, a brief analysis is presented here for the purposes of the threat model.

To prevent these users from hacking DTV tuners, the BPDG has released a set of robustness requirements for consumer electronics. The standard demands that a compliant device must "effectively frustrate" attempts to circumvent it (Perry, Ripley, & Setos, 2002). These include various requirements, such as ensuring that all buses are encrypted, and that all integrated circuits are soldered, not socketed, to boards. The requirements even go as far as naming screwdrivers in a list of tools that cannot be used to defeat the copy protection system in DTV products (BPDG, 2002). These countermeasures are likely to deter many people from finding weaknesses in DTV systems. However, the cost of consumer electronics must be kept low to ensure the affordability of these devices. Good hardware security is expensive. The BPDG realizes this, and has decided to forgo any countermeasures that would deter hackers using more sophisticated tools, such as logic analyzers.[3] Herein lies a sticky problem pointing to the weakness in the broadcast flag implementation: the system should be secure when distributed to millions of people, but should also be cheap.

The BPDG may feel that adversaries with logic analyzers do not pose a significant risk because of the limited number of people with both access to logic analyzers and the technical knowledge with which to hack DTV systems. However, one person who defeats copy protection on a DTV device may be able to share enough information about the method for others to circumvent copy protection on identical devices. Indeed, a similar situation existed with Microsoft's X-Box game system, which was designed to execute only Microsoft-authorized (digitally signed) code. In 2002

[3] A logic analyzer is a test instrument used for developing, debugging, and maintaining digital systems. It can record the electronic output of a hardware device to understand how the information flows through that system. It is a critical tool for reverse engineering.

MIT graduate student Andrew Huang, having spent many hours in a well-equipped lab, successfully crafted a method to run unsigned code on the X-Box. While not everybody has access to logic analyzers, the directions and information Huang (2003) provided helped others to run unsigned code on their own machines.

Developing a workaround for the copy protection on a broadcast flag-compliant device is not the only way to move movies to a computer. Another method, which may be much easier, is to use a DTV receiver that simply ignores the broadcast flag. Legislation will obviously make it illegal to import these devices from overseas, but US law cannot prevent their manufacture overseas. Even if international standards and self-regulation close off that source of new non-compliant devices, there are over six million HDTV devices sold to date. Many of these contain non-compliant decoders and digital outputs. There is no reason not to expect a flourishing black market in these devices under an enforced broadcast flag regime.

The BPDG is taking care to deter nefarious users from hacking broadcast flag-compliant devices by having robustness rules for compliant devices. However, given the availability of non-compliant technology, the determination of technically oriented nefarious users and the low threshold of file availability necessary to spread content, this group poses a high threat to the content industry's goal of blocking Internet distribution.

4.1.3. Organized crime

A third impediment to MPAA's goal of stopping Internet distribution of its digital content with the broadcast flag is organized crime. While most nefarious users do not have monetary gain as motivation to distribute movies on the Internet, there are groups whose motivation is of a distinctly monetary nature. These groups are analogous to the groups that currently copy movies and sell them on VHS tapes or DVDs on city streets, often based in off-shore operations. Since these groups have more financial resources than individual consumers, and can have factory-sized operations, it stands to reason that they will be more likely to succeed in an attack on breaking the copy protection technologies. The movie industry has identified illicit international organizations as a serious threat to its business model.

Any group with resources is more likely to have the technology necessary to circumvent the copy protection mechanism on DTV devices. Further, if they decided that HDTV was their preferred source for illegal content acquisition, exemptions in professional-level equipment would allow them to bypass the flag completely.[4] However, their profit motivation affects the likelihood that a group will actually distribute movies over the Internet. Instead, they will more likely use standard media such as VHS cassettes and DVDs, which do not offer HDTV quality. Moreover, the focal point of this large black market on first-run films (Valenti, 2003) makes the opportunity to down-market titles for broadcast over the public airwaves less appealing.

4.1.4. Threat analysis: illegal distribution

These tree possible groups have been previously identified by members of the content industry as threats with respect to content revenue. Of these three, the average users do not possess the technical skills or incentives to invest effort to circumvent the broadcast flag, or indeed, any

[4] "[regulations] will be crafted so as to exempt the requirements from applying to products that are specifically intended for professional and broadcast use" (Perry et al., 2002).

moderately sophisticated digital rights management scheme. Commercially organized actors ready to break the law will evade almost any protection, but are not interested in non-commercial distribution targeted by the MPAA. Sophisticated hackers, however, have demonstrated a desire to share files in the past, as well as a serious commitment to break complicated copy protection mechanisms. Since decentralized file-sharing systems do not require many input files for the widespread distribution of a file, the vulnerability of the broadcast flag to nefarious infringers leads to the conclusion that the flag will fail to protect this asset.

4.2. Goal 2: restriction of personal recordings of movies for time-shifting or library building

It is possible that content owners may be motivated by the broadcast flag's potential to limit individuals' ability to record movies for time-shifting or library building. Time-shifting is the practice of recording television shows for purposes of viewing them later at a more convenient time. Library building is the practice of recording television shows in a systematic fashion to keep from repeated viewing over a long period. These privileges go back to the Supreme Court decision *Sony v. Universal Studios* (1984), where Universal Studios sought unsuccessfully to show that time-shifting was a form of illegal copyright infringement. The court saw library building as a technical infringement, but not so severe a harm as to ban the technology since there was little commercial harm provable. However, *Sony* only dealt with illegal infringement issues—these privileges were not recognized rights but merely activities protected under the purview of fair use. The advent of the broadcast flag affords the MPAA an opportunity to effectively reverse the *Sony* decision in practice, if not in principle. While this is not a stated goal of the MPAA (they have, in fact, claimed the opposite[5]), it would appear to follow as a direct repercussion of the flag implemented across technology. Without an analog output on DTV tuners, the only way consumers will be able to record broadcasts is via copy-protected digital output. By creating the standards for broadcast flag compliance, the BPDG will be able to set restrictions on recording for time-shifting or library building. Given the past interest and technical potential, this can be considered an asset to protect control over content.

Practical subversion of this goal does not depend on how the broadcast flag is used. Indeed, it is easy to imagine uproar among consumers were they denied the right to record a favorite show. As a senior computer industry lobbyist noted, "…the more we restrict how our customers use our products, the more likely they are to be annoyed" (Black, 2003). This threat is judged on its full impact, and the power such control wields. By limiting how time-shifting and library building can occur, the content owners will have the ability to block previously established practices. These practices include making multiple copies, storing files on a variety of media and sampling video clips for alternate media uses. For example, a political speech broadcast on a news program under 'copy-once' could not be used for other purposes.

4.2.1. Independent individuals

Individuals working alone pose a threat to this goal if they are successful in circumventing the copy protection of a DTV system to make personal copies. These copies necessarily have to be

[5] "Q: When the broadcast flag is implemented, can I record any TV program…and watch it later…? A: Absolutely… Q: Can I make a back-up copy of that program for my library? A: Yes." (MPAA, 2002)

digital. This group is motivated by the desire to have the same capabilities in the new DTV world as in the analog TV world when such desires are thwarted by the limitations of Table A devices and "copy-once" compliance.

To be successful these individuals would have to reverse engineer a DTV tuner and/or digital recorder which, as noted above, will be difficult without specialized equipment. Regardless, their effect will be limited if they are not able to share this knowledge with others; the overall system still restricts copying for most of its users. Thus, independent individuals will not be successful in subverting the power of the broadcast flag to restrict personal recording of movies for time-shifting and library building purposes.

4.2.2. Malintentioned groups

Malintentioned groups with infringement in mind have as a goal circumventing copy protection in a way that is easy for others to replicate. Additionally, groups allow more widespread sharing of information than individuals. If fans of a particular broadcast program are unable to build a library as they wish, there might be a secondary market in reselling copies. Monetary gain could also be had if the group wants to sell modifications that disable copy protection. This would be similar to chip modifications of Sony Playstation video game consoles, allowing the modified systems to play games copied to CD-R disks. Thus, there is an incentive for malintentioned groups to attack this asset protected by the broadcast flag.

However, actions that would accomplish the circumvention of broadcast flag for this purpose would, like other circumvention efforts, violate the DMCA. This makes for a risky business model.[6] It may also be difficult to create chip modifications that work across systems. Unlike Playstation consoles, every model DTV tuner may be different. If we assume a heterogeneous market and variations in design and protection features, then attackers will have to work harder to subvert a large portion of the market. Security designers fear a system that is "break once, run anywhere" where knowledge of a single attack can be used to exploit any deployed system. This may not be the case with broadcast flag defenses.

Since consumers are not likely to take action by themselves to defeat copy protection, the larger threat is that someone will sell a service of modification to a DTV device to defeat copy protection. However, this threat is also not very significant because of the problem of charging for such a service. Under the DMCA this service is illegal, and the people involved in such businesses could be prosecuted, much as later game chip modifiers[7] have been (McCullagh, 2003). Thus, the threat of malintentioned cooperative groups in acting as a threat to MPAA's goal of restricting time-shifting and library building via the broadcast flag is low, not much higher than the threat posed by independent individuals.

4.2.3. Consumer electronic companies

If there are fewer ways to copy broadcast programming onto media, then demand may fall from people for whom library building and time-shifting is the primary reason for purchase. If this market segment is large enough, sales could fall. Consumer electronics firms would then be

[6] See 17 USC Section 1201 (a)(1)(A) "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."

[7] The original chip modifications to Playstations occurred prior to the DMCA.

frustrated with these restrictions and possibly seek some way around them to increase their market. Many consumer electronics firms, however, were active participants of the BPDG, and it is unlikely they would seek to undermine their own work. The question of participation and support for the broadcast flag among consumer electronics is further discussed below. The encouragement of regulation and penalties for violation makes industry subversion even less likely, so there is little threat of consumer electronics companies restoring the ability to make personal copies with impunity.

4.2.4. Threat analysis: library building and time-shifting

The movie industry has previously demonstrated an interest in controlling the flow of broadcast content beyond the point of broadcast. While such a right is legally protected where technologically feasible, the broadcast flag makes this control an asset that can be protected. This asset is successfully secured by the broadcast flag, since it does not require absolute effectiveness of control for the asset to be protected. Individual consumers cannot attack the flag themselves. Malintentioned individuals lack the ability to spread their skills effectively and they, along with consumer electronics firms, are legally deterred from making money from circumventing the flag's protection. The broadcast flag is effective security for control over how consumers can use broadcast content in their homes.

4.3. Goal 3: to protect new copyright paradigms

The broadcast flag can introduce a new paradigm in intellectual property control, where people do not see sharing as a natural right and content is completely controlled by its creator throughout its consumption cycle. This is an asset that the content industry has been loath to talk about in policy circles, but it stands to gain from such a shift. This new model can be threatened by consumers and government, but how exactly can the content industry benefit from a shift in the first place?

The current intellectual property paradigm is in flux. Most people simply do not consider the subtleties of infringement when they use copyrighted material. Whether making a mix tape for a friend or loaning a disk of software: their view of personal property is more flexible than that which the laws provide (Litman, 2001). Many in the content industry have observed that these permissive social views perpetuate casual infringement. As intellectual property lawyer Murray (1998) pointed out at a legal conference on copyright:

> So long as the general public believes that private copying for non-commercial use is not wrong in the digital environment, it is simply a given that we will see the immediate uploading and free downloading of best-selling novels, music, and - once the bandwidth is available—theatrical motion pictures by millions of people.

This casual view has logical roots. Litman (2001) observes that, historically, individuals have not personally encountered copyright issues in their daily life, as only publishers had to bicker amongst themselves to resolve copyright disputes. Prior to the digital age, most people could not publish, so were no more able to infringe on copyright than a rider on horseback can break the speed limit. The music industry has begun to fight this battle, with a website containing messages from recording artists about the losses they suffer from consumer

file-swapping.[8] Their strategy is to highlight the concrete harms caused by consuming a good that has zero marginal cost. The flag eliminates the need to make an emotional plea to change social mores, by altering what is possible. If something is impossible, public sentiment will not openly condone it: the paradigm shifts.

The source of the paradigm shift is worth noting. It will mark the first time that a coalition including content creators and copyright holders both dictate how the content can be used, and all as architects of the technological framework to enforce those decisions. To date, the copyright holder has not been able to prevent infringement. Instead, the copyright holder sues after infringement has occurred. Using the broadcast flag movie studios will be able to proactively restrict the use of their content.

4.3.1. Average consumers

Consumers, of course, are the foundation of the content industry's business model, and these consumers pose a threat to the MPAA's attempt to change the social perceptions on copyright infringement. If consumers were to speak out against the MPAA, or organize a large-scale boycott of movies because they were unhappy with restrictions on copying broadcast television, then the companies represented by the MPAA would be forced to answer. Consumer revolts over unwelcome copyright efforts are not unheard of. In the early 1990s, software firms used "dongles" or proprietary hardware attachments as a copy protection mechanism. Users had to plug tiny devices into their computers before the software could run: since only one such device came with the software package, users could not spread a single purchased copy among multiple machines. These dongles broke, were lost and created enough angry consumers that the firms stopped using dongles as a digital rights management system (Seymour, 1994).

Such a consumer revolt is not likely in the short run. Movies are, after all, popular. Moreover, as supporters of the flag point out, the restrictions on the average user *are* minimal in the short run, unlike the annoyance of software dongles or copy-protected CDs that will not play in standard players (Oakes, 2000). If initial reaction to the flag is tolerant, consumers will have a technological reminder that the content they are viewing is not their property in a standard sense: its uses are systematically limited. Just as ubiquitous flows of personal information can make some people resigned to an absence of personal privacy,[9] so too might a shifted technical reality change perceptions of use. This embedded lesson may shape thinking of intellectual property far more effectively than websites and artists' pleas.

4.3.2. Government

Congress poses a threat to attempts to reverse social perceptions with its power to codify certain rights under law. It has passed legislation condoning a freer perspective of musical content with the Audio Home Recording Act of 1992. The AHRA exempted consumers from lawsuits for copyright violation in certain cases in return for mandating copy protection mechanisms in home

[8] Musicunited.org is an industry-sponsored website that informs music listeners that file-swapping is illegal, that it hurts artists and that there are legal alternatives. Personal messages from popular artists themselves underscore lend moral credibility and authority to the ads. The campaign was launched with a full page New York times advertisement on September 26, 2002 (see http://www.musicunited.org/who_cares.pdf for the ad).

[9] As Scott McNealy, the CEO of Sun Microsystems, famously told Congress, "You have no privacy anyway…get over it."

audio recording equipment.[10] This balance is noteworthy, since it permits active user behavior that is technically infringement, but hides the content protection in a "natural" degradation function. It makes intuitive sense that a copy of a copy of a cassette might be less than perfect, just as is the case with a photocopy of a photocopy of a paper document. The broadcast flag, on the other hand, implements its protection in a more direct fashion, so that users will come to think that content simply is not *meant* to be copied and shared.

The AHRA was passed as a balance of competing forces and represented the interests of industries other than those aligned with the content creators, particularly consumer electronics groups. To strike a balance against the broadcast flag, similar coalitions would have to force Congress' hand. While this is always a possibility, it is not clear what stakeholders would rally to this coalition.

Similarly, Congress could be moved by public opinion to act, particularly if the administrators of the flag attempt to expand. An opponent of the broadcast flag has suggested that broadcasters might next demand prohibitions on fast-forwarding though commercials on taped TV shows (Black, 2003). Whether Congress would act is, of course, an open question. Certainly recent bills such as the DMCA and the Copyright Term Extension Act have tended to weigh in favor of copyright interests. Congress has not deviated much from its support of the content industry in the past two decades.

At the same time, the FCC might step in to attack the balance of power in the copyright debate. While the rulemaking process with respect to the flag has not indicated that they are inclined to mandate specific copyright protections, the possibility exists. The Commission could demand certain flag usage standards, for example, that force content owners to allow a certain number of copies, or allow some other fair use copying. The FCC might be interested in undertaking this to placate consumers unhappy about the DTV transition. Yet its interest appears at the moment to be primarily concerned with expediting rollout of the DTV infrastructure, and treading on as few toes as possible, rather than expanding its jurisdiction. In a statement to Congress, the chief of the Commission's Media Bureau stressed that it had "no desire to duplicate the work of the US Copyright Office" (Ferree, 2003).

4.3.3. *Threat analysis: copyright paradigms*

Policy is not manifested through laws alone, but can be embedded in technology (Lessig, 2000). The movie content industry can lock in new paradigms of copyright control with the broadcast flag, altering how consumers think about property, and tipping the locus of control from a balance between content owners and users to complete control by the content owners. If users do not protest at the beginning, this new paradigm will come to be a natural part of the technological landscape. There is scant evidence that legislative or regulatory agencies have an incentive to protest. If this new paradigm is seen as an asset to the content industry under the broadcast flag regime, there is little serious threat to it.

4.4. *Efficacy of asset protection*

As shown through the above threat analysis, the broadcast flag does not provide a robust technical solution to the problem of Internet redistribution of movies. It may serve as a "speed

[10] See 17 USC Section 1008 "No action may be brought under this title alleging infringement of copyright…based on the noncommercial use by a consumer…"

bump'' to prevent casual users from sharing files, but these users have never been the original source of content in networked distribution systems. The nature of existing online distribution chains such as peer-to-peer networks allow a ''break once, run anywhere'' model, permitting a few advanced users to crack the broadcast flag protection and then allowing others to share with impunity. The harms from sharing are, after all, not from the lost content, but forgone earnings from other consumers *accessing* the illegitimately distributed content, instead of paying for it themselves. However, the threat model does show that the broadcast flag will have a strong impact on average consumers of broadcast content, shaping how they experience and use it. It has the potential to prevent consumers from enjoying uses of content previously considered as ''fair uses'' in the analog realm, and to give content providers control over the use of their content. Though its stated goals are not met, the broadcast flag is a powerful security tool in defending these assets.

5. Constraints on implementation of broadcast flag

The above threat model made several assumptions which must be re-examined in the light of real world conditions to further assess the effectiveness of the broadcast regime. The threats to the assets of the content industry do not occur in a vacuum, but in the context of an information technology infrastructure and a business cycle for content. These starting conditions can influence how useful the flag is. For example, the ASTC transmission for a high definition signal streams out at 19.39Mbps. This is a massive quantity of data, even by today's standards, twice as large as the maximum throughput of the standard 802.11b wireless protocol. Even with some compression of the digital file, an hour's programming will create an 8–9 *gigabyte* file. For reference, a long song, encoded in MP3 format, will be less than one-thousandth of that size.

Why cannot this movie file be compressed, with its resolution reduced for easier sharing? Reducing the image quality would remove the impetus to protect the content as high definition, since a movie is available at many other places along the distribution chain before it is broadcast. Hollywood movies are currently broadcast over NTSC television standards, but these broadcasts occur at the very end of the distribution chain. Movies are released to different media to extract the maximum value from them, going from the theaters to VHS/DVD sale and rental to pay-per-view, through the premium movie channels before finally being made available on network TV (Dickens, 2003). At each of these stages, the content is vulnerable to capture for unauthorized distribution, whether it is a kid with a video camera in a movie theater, an Oscar judge looking for easy money, or a hacker ripping files off a DVD. All of these are known methods for retrieving files that end up on file-swapping networks. Moreover, it is unlikely that the content industry will alter this value chain to protect the content. Until this last stage, the consumer is willing to pay a premium to access the movie; in order for the market to shift, content owners must believe they can extract greater rents from the advertising-sponsored broadcasts than they can from other sources. While this may be possible due to the fantastic image quality of HDTV, it is not assured. Moreover, that quality will be present at the end of the distribution chain regardless of prior distribution. It is unclear what incentives would encourage studios to forgo the earnings from fee-for-service revenue channels by broadcasting films in DTV before DVD and video release. Any broadcast content will be vulnerable, under existing conditions, long before it is disseminated through the airwaves.

Even if these considerations were dealt with, the broadcast flag does not protect content from being captured from analog outputs and redigitized. This is the "analog hole" mentioned above. Relaxing this assumption actually weakens the security protections that the broadcast flag provides against library building and time-shifting—the content industry would have less control. However, it also completely obviates the flag as a protection against unauthorized capture of broadcast movies. As long as devices have analog inputs, there will be analog outputs, and the analog signal from that output can be captured and redigitized with fairly simple software packages. Once redigitized, the file can be distributed as if it were originally digital. While some image quality is lost in this process, the resulting file is certainly not unusable. As mentioned above, any HDTV-derived file will have to be "down-rezzed" to be sharable in the first place.

Each of these factors—file size, the distribution chain and the analog hole—mitigates the effectiveness of the broadcast flag as a protection mechanism. The large file size and vulnerable supply chain reduce flag effectiveness by reducing the need for a flag. This is similar to putting an expensive deadbolt on a house when the windows are left wide open, if high-resolution images are too large to trade in the first place, and low-resolution images are available elsewhere, content simply is not being protected by the flag. The analog hole exacerbates this problem by acting as a source of tradable files that can be of decent, if not high definition quality. Real world constraints prevent the flag from having its full effect as a security mechanism, particularly in the prevention of eradicating illicit file sharing. If the flag is built into most consumer devices, it may still hold as a defense of expanded powers for the owners and distributors of content.

6. Trade-offs and costs introduced by the broadcast flag

If implementing the flag can introduce a higher level of security into the system, it can also impose costs. Few systems are altered without some trade-off. Opponents of the flag have suggested three potential harms under a broadcast flag regime. Consumers may lose freedoms and abilities to which they are accustomed while incurring extra costs. As the FCC tries to mandate standards for technology, consumer electronics firms will be gaming to use compatibility as a competitive tool. Finally, if the flag mandates how devices can transmit data and interact with each other, future innovation may be stifled.

It is the consumers, in theory, for whom the broadcast flag is being set up. They are, by definition, the ones who will consume the content broadcast under the DTV regime, yet they also bear considerable costs. As part of the DTV transition, consumers will have to upgrade their broadcast television receivers. This does not necessarily include the high definition displays, which are a considerable expense, with or without a broadcast flag. Nonetheless, every set receiving DTV signals from the air must have a corresponding receiver. The broadcast flag regime regulates this receiver: it can only connect to other digital devices in the secure prescribed fashion. Moreover, in order to have any hope of closing the analog hole, external receivers must be discouraged. This precludes the option of a convenient set top box, that could be cheaply manufactured with demodulators and a standard output. Instead, consumers will have to purchase a new television that either contains an embedded demodulator or has a compliant digital input. The expected marginal cost of the broadcast flag to consumers is in the difference of a cheap conversion with a set top box and the more expensive integrated solution. Furthermore, all peripheral devices that

touch the content, including home recorders and projectors, must be upgraded. Any content leaving the demodulator would have to go to compatible devices that will honor the flag. Since none existed in the marketplace until very recently, consumers will have to purchase new devices to handle this digital content. Moreover, any newly recorded digital content will be encrypted and thus useless in legacy equipment. In total, the flag would pose a considerable expense independent of the HDTV transition.

Beyond the immediate fiscal cost, all consumers face an encroachment on fair use, as is briefly mentioned above. The authors of this paper do not wish to wade into that legal debate, often filled with passion and hyperbole. However, many consumers take advantage of the fluid nature of information under fair use on a regular basis. Consider the teacher who wishes to share a brief television clip with his or her class. The teacher must not only hope that the school's devices are modern enough to properly decrypt the flagged content, but may not be able to lend the clip to a colleague if the flag is set to disallow multiple views. Even if the flag is not set, that colleague must be local, since an e-mail client can hardly be considered a secure device. It is further worthwhile to note that a regime designed to protect fair use would not include a 'copy-never' flag at the broadcast level.[11] If set, this would effectively remove any ability to consume content apart from its direct broadcast. Consumer groups have also raised concerns, specifically on the question of who will determine what acceptable fair use comprises (CDT et al., 2002). Consumers face considerable real fiscal costs and a threat of diminished rights over what they can do with publicly broadcast content.

Manufacturer of consumer electronics, in general, will benefit from DTV transition, as more consumers buy devices that can handle digital signals. The broadcast flag introduces a new degree of compatibility, as devices not only have to be able to understand the ATSC signal, but must scan for the flag and encrypt digital outputs. This encryption is *not* mandated by the FCC, but is left to the implementer of the compliance standard. Standards are critical for interoperability in information systems, but can also be used as competitive weapons. An early market leader can capture the entire market, since late-entering consumers will seek devices that are compliant with the dominant technology. In the case of the broadcast flag, the 5C firms have been the first movers in putting forward technology that is endorsed by the BPDG's final report. Other firms face a time lag, the hurdle of the authorization process and potential complications from licensing agreements as obstacles to entering this new market. Non-5C firms are at risk from this process. Philips Electronics, for example, has developed an independent Open Copy Protection System (OCPS) that has been "rejected for inclusion on Table A at this time" by MPAA companies. The Consumer Electronics Association, whose constituents derive substantial revenue from television content devices, has repeatedly stressed that "copyright owners must resist the temptation to restrict technology" (CEA, 2004). Imposing controls on how information can be transmitted can limit competition among the manufacturers of existing consumer electronics.

Controls on information transmission can also limit future innovation. Information technology activist groups such as the Center for Democracy and Technology and Public Knowledge stress

[11] Richard Lewis, CTO of Zenith Electronics noted in a Congressional hearing the "As recently as last week, a large cable operator in an urban market had marked all digital content as "Copy Never", preventing digital recording of any kind" He cited this source in his written testimony: "Cablevision in New York City", *San Jose Mercury News*, September 18, 2002.

the value of an open network as a key asset of the Internet. Internet innovation is possible, the argument goes, because bits in a data network can be used for any function, and to limit which streams of data can be read by certain devices may curtail future innovations. Making devices "untamperable" and forcing devices to inspect incoming and outgoing data streams will prevent innovative users and entrepreneurs from developing new uses and products for existing devices. This is particularly true for general-purpose computers. As content converges to digital standards, developers seek ways to integrate these data streams. To comply with the broadcast flag, either PCs would be forbidden from touching flagged content, or secure PC platforms must be used. These platforms would necessarily have to prohibit user tampering with the data streams, turning a general-purpose machine into a content-viewing device. This obstacle to future innovation has captured the attention of Silicon Valley entrepreneurs who have come out against the flag (Wagner, 2004).

History has already shown that existing industries will attempt to stifle innovation for a perceived competitive advantage. Older industries often reap great benefits from technology they opposed at its onset, particularly in the content industry. After fighting the personal video recorder in *Sony*, the movie industry went on to turn the home video market into a substantial portion of its revenue. Home theater systems may well integrate with home information networks in the future, since all content will be digital and substantial data processing may be required. Implementers of the flag have not yet dealt with how content can be shared over a network without undermining the entire flag infrastructure. Yet if the flag prevents content from entering standard home networks, this will write off a large potential market.

The implementation of any security system involves trading security for other values, and the broadcast flag is no exception. It imposes concrete fiscal costs on consumers, and presents substantial risks to consumer fair use rights, consumer electronic competition, and future innovative potential in the information technology industry. Understanding these trade-offs in the context of the original security question is critical.

7. Conclusion

Any policy maker, when faced with a proposed course of action, must determine whether it is good policy and, to that end, must find the appropriate tools for analysis. This paper approaches the contentious proposal of the broadcast flag with the computer security tool of a threat analysis. The flag was originally proposed to protect digital broadcast content from unauthorized distribution across the Internet, but it can also be seen to protect an increase in the ability of content owners to control how consumers use time-shifting and library building, and defend a shift in the paradigm of intellectual property so as to be closer to a real property model. The threat analysis found that this first goal was vulnerable to an attacker who did not need a high rate of success to subvert the goal of keeping content off the Internet, especially in light of the conditions in which the flag would be operating. The latter goals that more subtly aided the content owners were better served by the broadcast flag. The final aspect of the threat analysis identified substantial costs of implementation borne by those who were not direct beneficiaries of the security protection of the flag.

This analysis concludes that the explicit goal of broadcast flag proponents is not realistic, whereas those that might be more feasible are more subject to controversy. At the same time, the costs borne by consumers and the risks of future harms to consumer rights and future innovation seem a high price to pay for the protection of these assets. Embedding digital rights management into the broadcast television infrastructure when so much is at stake and so little is to be gained probably is not good public policy.

Acknowledgements

The authors must thank Barb Fox and Hal Abelson for their invaluable guidance and feedback, and Mike Godwin for his valuable input. They are also grateful for the comments of Robert Cannon, Beau Kilmer, Adam Thomas, and an anonymous reviewer.

References

Adar, E., & Huberman, B. A. (2000). Free Riding on Gnutella. *First Monday*, *5*(10). http://www.firstmonday.dk/issues/issue5_10/adar/.

Black, E. (2003). *Privacy prevention and the broadcast flag*. Testimony to the House Committee on the Judiciary, Subcommittee on Courts, the Internet and Intellectual Property, March 13, 2003.

Broadcast Protection Discussion Group (BPDG). (2002). *Draft compliance and robustness requirements document* (Copyright Protection Technical Working Group http://www.cptwg.org/html/Bpdg_home_page.htm).

Center for Democracy and Technology (CDT), Consumers Union, & Public Knowledge. (2002). *Consumer policy questions and issues regarding the BPDG proposal for protecting DTV content* (memo to House Commerce Committee Staff, July 10, 2002. http://www.cdt.org/copyright/020719bpdg.pdf).

Consumer Electronics Association (CEA). (2004). *Protecting consumer home recording rights*. CEA Position Paper.

Dickens, J. (2003). DVD hits the big time. *Mercer Management Journal*, *15*, 77–82.

Ferree, W. K. (2003). *Copyright privacy prevention and the broadcast flag*. Testimony to the House Committee on the Judiciary, Subcommittee on Courts, the Internet and Intellectual Property, March 13, 2003.

Goroch, A. (2001). HD in the clouds? DBS seek to stay ahead, despite slow growth in HDTV. *Broadband Week*. Posted January 22, 2001. http://www.broadbandweek.com/news/010122/010122_wireless_hdtv.htm.

Hachman, M. (2004). Powell riffs on DTV, wireless, regulation. *PC Magazine*.

Huang, A. (2003). *Hacking the Xbox*: *An introduction to reverse engineering*. San Francisco: No Starch Press.

Joseph, J., & Miller, J. (2003). *Digital television sales flourish during first half of 2003*. Consumer Electronics Association Press Release. (http://www.mpaa.org/Press/Broadcast_Flag_2A.htm)

Lessig, L. (2000). *Code and other laws of cyberspace*. New York: Basic Books.

Litman, J. (2001). *Digital copyright*. Amherst, NY: Prometheus Books.

McCullagh, D. (2003). *US crime-fighters seize web sites*. CNet News.com. Posted February 26, 2003. http://news.com.com/2100-1023-986225.html.

MPAA. (2002). *Broadcast flag frequently asked questions*. Motion Picture Association of America.

Murray, C. (1998). Discussion—technical measures and anti-circumvention. Proceedings from the intellectual property system major problems conference. *Journal of Law and Technology*, *39*, 291–387.

Oakes, C. (2000). Copy-protected CDs taken back. *Wired Magazine*. Posted February 3, 2000. http://www.wired.com/news/technology/0,1282,33921,00.html.

Patrizia, A. (1999). DVD piracy: It can be done. *Wired Magazine*. Posted November 1, 2001. http://www.wired.com/news/technology/0,1282,32249,00.html.

Perry, R., Ripley, M., & Setos, A. (2002). Final report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group.

Philips Inc., Thomson Inc., & Zenith, Inc. (2002). Comments on the final report of Broadcast Protection Discussion Subgroup.

Nielsen Media Research. (2001). *Nielsen Media Research Estimates 105.5 million TV households in the US*. Nielsen Press Release.

Schneier, B. (2003). *Beyond fear*: *Thinking sensibly about security in an uncertain world*. New York: Copernicus Books.

Seymour, J. (1994). Dongles foil pirates-but drive users crazy. *PC Week*, *16*, 44.

Smith, S. (2003). From Napster to Kazaa: The battle over peer-to-peer filesharing goes international. *Duke Law and Technology Review*, 0008. http://www.law.duke.edu/journals/dltr/articles/PDF/2003DLTR0008.pdf.

Sony v. Universal Studios 464 US 417 (1984).

Valenti, J. (2003). *International Copyright Piracy: Links to organized crime and terrorism*. Testimony to the House Committee on the Judiciary, Subcommittee on Courts, the Internet and Intellectual Property, March 13, 2003.

Wagner, J. (2004). Broadcast flags scorned by Silicon Valley. *Internet News*. Posted March 15, 2004. http://www.internetnews.com/xSP/article.php/3326341.