

Will the broadcast flag interfere with consumers ability to make copies of DTV content for their personal use, either on personal video recorders or removable media?

The ATSC "broadcast flag", if implemented and mandated, will unquestionably interfere with the ability of consumers to make copies for personal use. It is similar to the SCMS copy management system already mandated by Congress for digital audio recording equipment under the Audio Home Recording Act (AHRA) of 1992. The broadcast flag, when set, would state that content could not escape its current viewing system, similar to how the SCMS flag (when set) prohibits making any future generation copies of a work. However, the broadcast flag is much more omnimous in that it would prohibit external copies from ever leaving the system that created them.

The problem with captive systems such as these is that over time, they get replaced. Furthermore, technologies evolve over time. Consider the woe of someone who owns a collection of 78 RPM vinyl records; modern record players are nearly identical to those capable of reading the 78 RPM format, but still will not play them!

Given that all recording mediums decompose over time, someone trying to preserve their grandparent's music from the 1940's might first record have rerecorded it to reel-to-reel tape during the 1960's, then to cassettes in the 1980's, then to CD-Rs in the 1990's. Soon they will record it to a format to be determined during the upcoming century before their CD-Rs get damaged, or start to "bit rot." Without the ability to copy works freely as described above, one has to rely on a commercial provider to license the rights to reissue an item for public sale and "digitally remaster" the work for a modern audience, which may or may not occur. (During all the above coping, no illegal action has taken place; all of these actions are considered licensed and/or fair use.)

In the short term, it is worth noting that many modern consumer products only are designed with a 4-5 year expected lifespan at best. If someone has their digital recorder hold a broadcast-flagged work captive, and the recorder dies 2-3 years down the road, said owner is going to be annoyed, with no recourse or inexpensive way to remedy the situation.

Would the digital flag interfere with consumers ability to send DTV content across networks, such as home digital networks connecting digital set top boxes, digital recorders, digital servers and digital display devices? The ATSC flag in question, if implemented, will create significant problems for consumers connecting various devices together, whether by a network or other media. This will occur for a number of reasons. Since the broadcast flag will require content to be protected, but not state every last detail of how to implement said protection, manufacturers of different devices likely will start using different protocols and methods to do so.

Already, there are a myriad of digital standards used to connect equipment together. While some of these are popular (Firewire, SPDIF, etc.), they often vary in terms of connectors used (Firewire has two connector sizes; SPDIF can be implemented electrically two ways, or optically), what they carry (MPEG 2 versus MPEG 4 data; etc.), and are called different things by different manufacturers (IEEE 1494==Firewire==i.Link). Popular protocols sometimes also have vendor-specific "flaws" or "enhancements" in them that may prohibit data from transferring between devices of different

manufacturers. Some vendors may choose to implement one popular protocol, others may implement two or three; it all depends on the manufacturer's preferences and what the trend is at the time.

In addition, manufacturers often come up with their own digital protocols.

The reasons for this vary; sometimes no similar protocol exists, sometime they just want to, and sometimes the protocol is used to supplement another, or provide additional functionality (such as a Brand X Compact Disc player being able to tell a Brand X audio amplifier to switch to the CD input when its user presses "Play"). These vendor-specific protocols often have a very limited lifetime, significantly limiting the usefulness over time of their implementing devices.

Without every last detail of how content would need to be protected mandated by the FCC, implementation of the broadcast flag likely would have different groups of vendors doing different things. While this is not necessarily new, the fact the ATSC flag might prohibit a consumer from upgrading to a competitor's system without losing their recorded television programs, and this is a major concern for Americans as a whole.

Would the broadcast flag requirement limit consumers ability to use their existing electronic equipment (equipment not built to look for the flag) or make it difficult to use older components with new equipment that is compliant with the broadcast flag standard?

There are two cases we have to consider to answer this if the broadcast flag would affect equipment already in the hands of consumers. Antiquated analog and antiquated digital equipment likely will be treated differently, as the later can create a "perfect copies" more likely to annoy content makers.

Analog Equipment:

Analog equipment, in theory, should be able to interact with the new digital equipment within certain tolerances. However, this is not 100% true. First of all, the Digital Millennium Copyright Act requires analog video recorders to be unable to record signals "scrambled" with a system such as Macrovision. Theory states this should be fine, as this concept can enforce the broadcast flag.

In practice, the makers of many digital devices with analog video outputs set their outputs as "dumb," constantly scrambling the signal. Buyers of new digital products will not be able to determine how a manufacturer implements this with respect to the ATSC system until they purchase and use a product.

Second, we must consider how long new equipment with analog outputs will exist, as previously described. While there is quite a legacy of NTSC equipment backward compatible to the black & white televisions of the 1940's, I do not foresee analog compatibility remaining for more than 10 to 15 years. "Video input" jacks only started appearing on television sets in the late 1980's/1990's, and S-Video jacks only became commonplace after DVD video players were out.

Finally, I wish to note that while it may be possible to record in an old analog source, it is likely that many digital devices may lack analog outputs to do the reverse. This is a problem for the reasons described in

response to Question #2.

Digital Equipment:

It is unlikely that any old digital equipment will be able to receive outputs from digital devices that respect the broadcast flag, as they are considered "insecure" by many parties. Setting the the SCMS "copy" flag that already exists to prevent future duplication does not compensate for the fact that many current professional-grade and "prosumer" devices can be easily set to ignore these.*

It is likely that at least some new digital devices will be able to import older digital formats into them. But after the first generation or two of broadcast flag respecting devices are out, it is unlikely that many will have this ability.

Some devices, erring on the side of copyright holders, might allow content to be imported into a new recording standard, but mark that said content may then never leave the new standard for a future one. This could have a major impact on fair use, as future generations would not be able to use access older content at all.

*For example: Many widely available Digital Audio Tape (DAT) decks on sale today for about US \$1000 can be told to ignore SCMS. This is not out of disrespect for the law; rather, the people who typically own them often need to bulk copy and/or "mix down" their own original works.

Most protection schemes on existing computers are done purely in software, and hence can be easily bypassed. The solution to this (Microsoft's Pallidium, et. al.) may be worse than the symptoms.

Would a broadcast flag requirement limit the development of future equipment providing consumers with new options?

It is hard to say if the broadcast flag would prohibit the consumer from receiving new options and/or innovations. The large manufacturer definitely would be able to create new devices using the broadcast flag, as they can easily implement the protections mandated by the standard.

However, it is worthy to note that the broadcast flag definitely would cause problems for small development businesses, students, researchers, and casual tinkers. And it is these parties that are typically considered to be those that drive innovation.

Consider the case of a person wanting to build their home theater from scratch. Heathkit sold large-screen television kits during the 1980's, so building one should still be possible. Readily available schematics exist for AM/FM radios and audio amplifiers. Consumer-grade drills, saws, etc. can be used to build a record player, cassette deck, and the VCR given the proper parts.

Now all this person needs is their modern CD and DVD player. Can someone build these on their own?

CD & DVD players require mechanical tolerances much tighter than those possible in the average home machine shop. Given a prebuilt disc carriage,

the CD player might still be possible. As per the DMCA, a DVD reader requires numerous copyright checks and enforcements to be made. Could a small party implement these?

The licensing fees to even gain access to the DVD standard with its encryption schemes, etc. needed to read DMCA-enforced DVD discs is \$15,000 per year, assuming I am reading the DVD CCA's web page correctly. This cost is prohibitive to all but the largest firms. Reverse engineering it for interoperability would require high-speed data acquisition equipment, time, and a lot of other resources; for the cost of these, you might as well pay the licensing fee.

There is no way for a student, casual tinker, researcher, or small firm to brew their own DVD system or fully study how an existing commercial model works without licensing all the protocols and techniques used, since copyright law and implementation agreements prohibits such devices from being easily traceable. All the end user can see is that encrypted bits go in, and encrypted bits go out.

The broadcast flag will mandate that all video equipment be put into the situation that DVDs are today. Future generations will not be able to learn how any video equipment works by taking it apart, which will definitely stifle innovations devised by smaller parties.

What will be the cost impact, if any, that a broadcast flag requirement would have on consumer electronics equipment?

The cost impact to implement the broadcast flag equipment likely will be minimal due to sheer bulk volume. Even if a device needs dedicated circuitry to perform implement ATSC, the bulk cost of electrical components purchased by the thousands if not millions will likely drive said cost to \$20 per unit or below.

Of more concern is the fact that while everyone likely will support the new digital television format, only a limited number of manufacturers will support each inter-device interconnect method, and the interconnection method of choice may change over time as devices improve. This may or may not lead to higher costs of ownership as long-term users of the losing standard(s) encounter usage barriers.

Other Comments:

1. All media copy protection systems operate on the principal that an end user is a thief. To that end, they then attempt to define what "fair use" is for a work by limiting what can record an item, how long it can be played, how many future copies can be made, etc.

Unfortunately, all conceivable fair uses cannot be decided ahead of time. It may be necessary to make a backup copy of a backup if the original fails, or to copy between several different types of recording mediums as time progresses. In order to write a movie review, an Internet reporter might consider a 30-second clip of a movie marked as uncopyable as the most representative of the movie as the whole, while the movie's producer only marks a different, 15-second segment as suitable for use in a review.

No copy management system currently in existence allows users to do the above. And no copy management system likely can allow such without without

risking abuse. Watermarking and/or keying content to specific users limits problems somewhat and can allow free distribution, but if a user's key is compromised, there is no way to prove who compromised it, and revoking the user's right to use works they purchased might be considered ethically incorrect.

Instead of trying to introduce new regulations which reduce the rights of consumers, the parties concerned that their works will be illegally copied should take advantage of existing laws to prosecute those violating their copyrights. Recently, the Danish Anti-Piracy Group (APG) did a rather unique legal maneuver*, and billed people for their allegedly illegal peer-to-peer use, forcing them to court if they did not pay. The talk about this action alone has caused a number of people to stop using peer to peer networks illegally.

U.S. anti-piracy groups would be wise to take a page from the danes' book instead of complaining that going after the illegal activities of end users is "cost prohibitive." By not prosecuting certain classes of illegal actions, they are defacto implying that such actions are legal, and then wondering why they have problems.

* Warner, Bernhard (Reuters newswire). "Anti-piracy group orders Net downloaders to pay up." November 26, 2002, last viewed December 5, 2002. Available online:
http://digitalmass.boston.com/news/2002/11/26/anti_piracy.html
(and elsewhere).

2. Table A of the BPDG report lists a number of potential protection systems that could be used to enforce the ATSC flag. Many of these use different types of encryption, and are incompatible with each other. Furthermore, some of these, such as the Content-Protection for Recordable Media (CPRM), require "unscreened" content (presumably that the system does not know the copyright status for, such as items being imported from legacy video systems) never to be copied again.

Changes of encryption schemes might as well be considered changes of media, and changes of media are much more common than many people realize. Consider the "super floppy wars" during the 1990's meant to replace 3.5" computer data disks with a modern equivalent. There was Iomega's Zip 100, which was popular, but not backwards-compatible. There was the LS-120 (now "Superdisk") format, which was backward compatible and had several manufacturers, but was not very popular. And there was Sony's HiFD format, which could hold more data (200 MB) than its competitors of the time, but never took off in any manner whatsoever.

Today, if you hand the average user an LS-120 disk, chances are better than 99% that they will not have a reader for it, nor know anyone that does. If you hand a user Zip 100 disc, there is a significantly better chance that they will be able to read it or know someone who can, but users of Zip 250 and Zip 750 drives cannot write to said media in a manner that an "old" Zip 100 drive owner can read.

Only two of these three formats being sold to consumers still exist, one of them only barely. And these formats are all less than 10 years old! Even within a media, formats on the media change; Compact Disc players have to deal with the original CD format, CD Xtra, CD-R, CD-RW, etc., while DVD players have to deal with the original DVD format, DVD-R, DVD-RW, DVD+RW,

and others (some current players not even implementing all of the above).

If the ATDC flag is even implemented slightly improperly, consumers will be severely impacted as they upgrade their equipment and/or video recording collections. But if the FCC only allows one type of ATSC implementation for all time, that may stifle innovations that go against what said implementation allows, as well as prohibit consumers from importing their content marked "no future copies" to the next digital television standard.

3. Professional video "pirating" groups will always be able defeat security systems such as the broadcast flag. This flag will only really effect end-users, which many groups consider the least of the media industry's problems.

In order to make life harder for professional pirates and/or "ban" devices later found to be flawed (making their owners unhappy), encryption must be incorporated alongside the transmitted signal, making ATSC implementation much more complex at transmitting stations. Starting encryption at the receiver end means that the radio signal transmitted is unencrypted, allowing a hostile parser to record the digital movie without any restrictions anyway.

4. The ATSC/broadcast flag could be considered a modern equivalent of telling everyone in the United States not to make or sell radios that can receive cellular phone conversations. Outside of the United States, there are no such restrictions, effectively degrading said restrictions in the U.S.

5. Video recorders set to record broadcast flag protected shows would not know if they could record such a work until said work was on television, and the recorder attempted to record said program. If the flag stated that the program could not be recorded at all, a person attempting to record said program on a timer might later come back to find quite a shocking situation.

6. The author is a "special-status"* Ph.D. student in Electrical Engineering at The Ohio State University, as well as a licensed amateur radio operator, tinkerer, and a certified professional engineer-in-training. This document is an independent work, and nothing in this document should be considered to be the policy nor view of said university.

* Master's Degree granted at another institution.

7. All trademarks appearing in this response are owned by their respective trademark holders.