Lessons of the FCC Broadcast Flag Process

Background for the Legislative Debate
September 2005

A federal appeals court vacated the FCC's broadcast flag rules in May 2005, putting the question of whether to authorize a flag regime back before Congress. A close examination of the FCC flag proceedings prior to the court's decision offers important lessons for the legislative debate. Even though the FCC approved as "flag compliant" all 13 technologies it considered, the nature of the approval process led technology companies to withdraw valuable product features under pressure from third parties. This demonstrates that a flag regime does indeed carry risks to innovation, as some critics of the flag have argued. It also suggests that the structure of any approval process is crucial. If Congress elects to reinstate a broadcast flag regime, it should take care to guarantee that the process will be open, predictable, and will avoid preferential treatment for technologies endorsed by particular industries or established companies.

Introduction

On May 6, 2005, the United States Court of Appeals for the D.C. Circuit threw out the Federal Communications Commission's (FCC) "broadcast flag" rules on the ground that the agency had no statutory authority to adopt them. Supporters of the broadcast flag therefore are asking Congress to provide the authority the court found lacking.

CDT is not endorsing the position that Congress should provide such authority. We do, however, believe that important interests are at stake. Content creators argue that technology-based protections will help them feel comfortable releasing their works in new forms, including on the Internet. At the same time, content protection tools may impact the public interest in the development of new technologies that empower consumers and the public's access to news, information, and other content through the Internet and other digital networks of the future. Decisions concerning whether and how to implement a broadcast flag regime will determine what technologies are allowed not only in digital televisions but also in computers and other devices and what uses consumers are able to make of digital video content.

The FCC's broadcast flag process from 2002 to 2004 provides significant context for this ongoing policy debate, showing the risks of a flag regime that lacks standards and procedures to protect the public interest.

The FCC's rules would have required all consumer products that handle digital television, from TVs to TiVo digital video recorders and from DVD recorders to personal computers, to include some type of approved technology for recognizing and protecting flagged content. The FCC allowed companies to propose different content protection technologies, and conducted the initial round of the approval process. The record of this proceeding offers insight into how the FCC's broadcast flag regime was shaping up to work in practice.

The FCC considered and ultimately approved thirteen proposed technologies. Most of the controversy during the proceeding centered on a secure networking technology proposed by TiVo and opposed by content companies. TiVo's approval, along with that of a similar technology called SmartRight, represented a victory for groups that had urged the FCC to keep the broadcast flag narrowly focused on protecting digital broadcasts against massive indiscriminate redistribution online. The FCC refused to expand the agreed upon scope of the flag rules to preclude use of the Internet with digital television (DTV) devices. The agency was rightly applauded for its decision.

The FCC's final determinations on TiVo and SmartRight were only part of the picture, however. One of the most important untold stories of the approval process were the decisions of consumer electronics and IT companies to withdraw valuable proposed features from their products under pressure from third parties, before the FCC ever had a chance to rule. In several instances, the flag process gave the content industry undue influence over the technology offerings of several technology applicants, allowing it to shape product design in areas outside the explicit scope of the rules.

The creation of any significant new regulatory regime – especially one that affects rapidly evolving technology industries – raises concerns that over time the regulatory approval process may be used by established companies in the regulated industry or by third parties with related interests to protect established market interests or block disruptive technologies. The history of the first round of the flag process suggests that, as the regime was implemented in its first trial phase, it was susceptible to this kind of misuse.

In a separate document ("Broadcast Flag Authorization Legislation: Key Considerations for Congress"), CDT has outlined recommendations for safeguards Congress should include if it chooses to proceed with broadcast flag authorization legislation. Several of those recommendations relate to providing clear parameters and procedural requirements to govern the FCC's process for approving "flag-compliant" technologies. This paper demonstrates that the history of the FCC's initial approval process provides strong support for these recommendations. Based on the experience of the FCC's first effort at implementing a flag regime, it is clear that an FCC approval process could chill

valuable new communications technologies for consumers and Internet users – even when no technology is expressly rejected. The paper concludes with suggestions for minimizing this risk, by making the approval process more open and predictable and by avoiding preferential treatment for technologies endorsed by particular industries or established players.

CDT looks forward to working with all interested parties as Congress considers whether and how to authorize the FCC to implement a broadcast flag regime.

Background

The "broadcast flag" was proposed to the FCC as a way to protect DTV broadcasts from massive redistribution over the Internet. DTV is slated to replace the analog broadcasts received by most existing televisions in the United States, and Congress is currently debating a possible "hard deadline" to complete this transition within the next several years. However, content owners said that they would be unwilling to release valuable content for high quality digital broadcasts unless there was some assurance it would be protected from massive redistribution. Thus, in November 2003 the FCC adopted the flag regulations with the explicit and narrow goal of "prevent[ing] the indiscriminate redistribution of [flagged] content over the Internet or through similar means."

Under the regulations, broadcasters would have had the option to mark or "flag" television programs with a small bit of code indicating that they were to be protected against widespread copying and redistribution. All new digital televisions and other devices that receive DTV content would have been required to include approved digital rights management (DRM) technologies intended to recognize the flag and help shield flagged programs from massive redistribution, and that would be robust enough to prevent hacking using generally available equipment. These rules would have affected TV sets, computers, DVD recorders, and digital video recorders (such as those manufactured by TiVo), all of which would have had to include government-approved technologies to display, transmit, or record marked DTV programs. CDT's December 2003 report, "Implications of the Broadcast Flag: A Public Interest Primer," provides an in-depth analysis of the policy implications of implementing a broadcast flag regime.

Because of the potentially sweeping impact of the flag regulations, there was substantial controversy surrounding their adoption. Critics worried that the flag regulations would serve as a roadblock to innovation, particularly in uses of DTV content on computers and online. Supporters of the flag responded that it was narrowly focused on preventing massive online piracy and would not

interfere with Internet technologies so long as they prevented widespread redistribution of content.[1]

Reflecting these arguments, the FCC's Order adopting the rules contained repeated assurances that the flag regime would be narrowly focused. The Commission repeated the phrase "indiscriminate redistribution" no less than thirteen times in its November 2003 Report and Order, reiterating the rules' narrow scope, and said that it sought to "facilitate innovative consumer uses and practices, including use of the Internet as a secure means of transmission."[2] The Commission wrote specifically, "we do not wish to foreclose use of the Internet to send digital broadcast content where robust security can adequately protect the content and the redistribution is tailored in nature."[3]

Important questions about how to implement these goals were left open by the Commission's initial ruling, however. When the Commission released the flag rules, it deferred the issue of exactly how protection technologies would be approved, who would make the determination, and according to what criteria. These questions, which would have determined what devices and capabilities actually would be available to makers and users of DTV products, were deferred to a follow-on rulemaking. That rulemaking was never completed.

Because some decisions had to be made immediately, however, the Commission adopted an "interim" procedure. Under this process, approval of protection technologies was to be determined by the Commission based on evaluation of a list of general factors. Ten companies submitted a total of thirteen proposals for approval under the interim process. Four of these, but particularly a proposal by TiVo, were the focus of substantial controversy.

After a five-month review, all thirteen technologies were approved on August 4, 2004. Consumer groups applauded the approvals, particularly the decision on the contested TiVo technology.

The record leading up to these approvals, however, includes evidence of serious flaws in the review process. Specifically, content companies exercised a great

---

[1] "The broadcast flag is intended to prevent the widespread redistribution of content. If technology exists to permit secure delivery of that content to your summer home or to your office, that is not something that the broadcast flag is intended to prevent, and presumably, it will not." (Testimony of Fritz Attaway, general counsel of the Motion Picture Association of America (MPAA), before the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property Oversight Hearing on "Copyright Piracy Prevention and the Broadcast Flag," Mar. 6, 2003.)

[2] FCC Report and Order and Further Notice of Proposed Rulemaking, MB Docket No. 02-230, In the Matter of Digital Broadcast Content Protection (released Nov. 4, 2003) ("Order/FNPRM") ¶ 10.

[3] Order/FNPRM ¶ 63.

deal of influence over the process, convincing several companies to drop exciting networking features before the FCC ever had a chance to review them.

The FCC wrote in the Order adopting the broadcast flag, "We are concerned with one industry segment exercising a significant degree of control over decisions regarding the approval and use of content protection and recording technologies in DTV-related equipment."[4] CDT believes that the first round of technology reviews in fact exhibited such undue control and that it would have been a serious ongoing risk associated with the FCC's process, had the rules remained in force.

On May 6, 2005, the U.S. Court of Appeals for the D.C. Circuit struck down the FCC's broadcast flag rules, holding that the agency lacked jurisdiction to regulate how televisions and other devices handle content after the broadcast transmission has been received. Therefore, if the FCC is to implement a broadcast flag regime, it will require express legislative authorization. If Congress considers legislation to authorize the FCC to implement the broadcast flag, it should learn from the serious shortcomings of the FCC's initial flag proceedings and structure any approval process carefully. In a separate paper, "Broadcast Flag Authorization Legislation: Key Considerations for Congress," CDT has listed specific recommendations for safeguards Congress should include if it chooses to proceed with flag legislation. This paper looks backward to draw lessons from the FCC's initial effort to implement a broadcast flag regime.

The Proposed Technologies

Of the thirteen technologies submitted to the FCC for approval under the broadcast flag, four originally included specifications permitting secure transmission of recorded broadcasts over the Internet. These were Thomson *et al.*'s SmartRight technology, Real's Helix DRM system, Microsoft's Windows DRM system, and TiVo's TiVoGuard proposal.

These technologies would have allowed consumers to watch content recorded on one device from other devices at remote locations. For example, they would have made it possible to retrieve a show that had been recorded at home on a digital video recorder (DVR) and send it to a computer in the office for viewing there, or for parents to record a local high-school sports broadcast on their DVR and then send it to the DVR of their child at college. The features were

[4] Order / FNPRM ¶ 52.

proposed for inclusion in dedicated consumer electronics devices and in software running on a general purpose PC.

In order to ensure that the networking capabilities did not lead to massive redistribution, each technology included limits on transmissions:

- Microsoft's Windows DRM system would have allowed "streaming" of content, but not copying, and streaming would have been permitted only to a limited number of devices.
- Thomson would have allowed transfers, but only to a limited number of devices registered as part of the same "Personal Private Network."
- Real provided for a variety of protection schemes, including limits on the number of copies, limits on the number of simultaneous streaming connections, and limits on the ability to make second-generation copies.
- TiVo's proposal allowed transfers to up to ten TiVo DVRs or personal computers, provided all the devices were registered to same TiVo account.

In order to ensure the security of the system, all four proposals provided for robust encryption and the capacity to revoke an individual, compromised device's ability to send and receive flagged content over the Internet.

In sum, the creation of secure Internet connectivity in each of these devices provided for significant and novel personal uses of content. But in each case, these features were coupled with robust security protections, to allow content to travel over the Internet without exposing it to indiscriminate redistribution online.

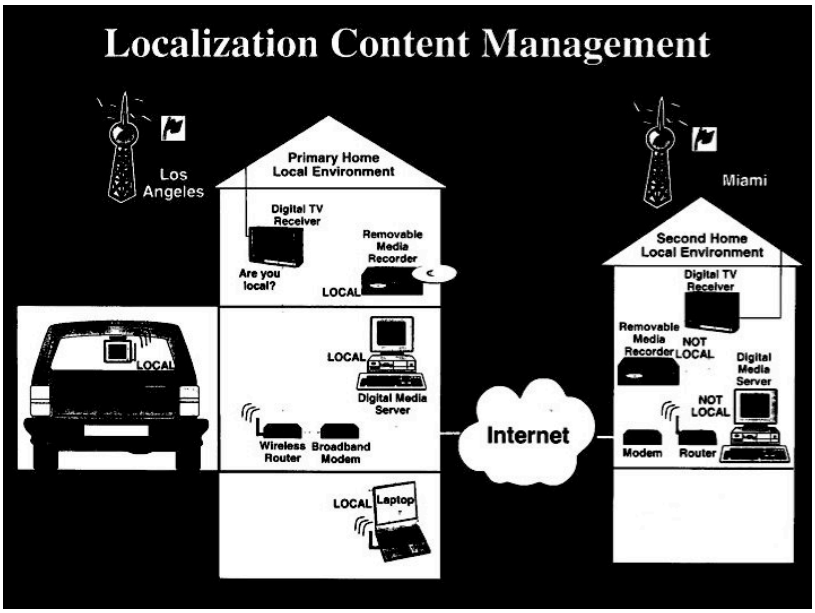
Opposition by the MPAA and Others

The Motion Picture Association of America (MPAA) filed oppositions to each of the four of the proposals. The MPAA raised a wide range of concerns, including questions about licensing terms and handling of revocation for compromised devices. The Association also reasonably requested several clarifications in the security features of the submitters. For example, while Microsoft and Thomson had indicated that the number of devices to which recorded content could be transmitted would be limited, they had not provided a specific upper bound. The MPAA reasonably argued that the submission should be required to contain an actual number for the limitation. Microsoft responded to the

MPAA's request for a specific upper limit on streaming devices by agreeing to set the cap at ten.[5]

However, the MPAA also argued against the fundamental idea of transmission over the Internet – even if security had been assured. Although the MPAA had originally asserted that the flag should focus on preventing indiscriminate sharing, and that secure online uses should be facilitated, the Association now proposed a new and much more restrictive standard: "localization" of content. The MPAA argued that preserving geographic divisions in broadcast markets was crucial to the businesses of its members. Therefore, the MPAA opposed any technology that did not "constrain unauthorized distribution beyond the . . . set of compliant, authorized devices within a tightly defined geographic area around [a DTV receiver]. For example . . . the set of authorized devices within or in the immediate vicinity (e.g., the yard, garage, or driveway) of [a] home."[6]

The MPAA illustrated this view in an *ex parte* presentation to the FCC:



[5] Consolidated Reply of Microsoft to Oppositions in Docket MB 04-66 (filed Apr. 16, 2004) ("Microsoft Reply") at ii.

[6] Comments of the Motion Picture Association of America, *et al.*, in MB Docket 02-230 (filed Feb. 13, 2004) at 7-8. In later submissions as part of the interim process, the MPAA slightly revised this position, saying it was not opposed to non-local transmission *per se*, but that this issue required further study, and the Commission should delay approval of features that allowed non-local transmission pending further study of the issue. *See, e.g.* Opposition to the Application of TiVo for Interim Authorization of TiVoGuard by the Motion Picture Association of America, *et al.*, in Docket MB 04-63 (filed Apr. 12, 2004) at 3. CDT's view was that the Commission had already answered the question of the scope of the flag – and therefore the issue of localization – in its initial Order. A localization requirement clearly would have been an expansion of the flag rules, and therefore no further study was needed to see that it was inappropriate.

The MPAA's revised standard would have ruled out transmission over the Internet.

The MPAA was joined in opposition by the National Football League and Major League Baseball. Both objected that transmission over the Internet would hurt their stadium revenues. The leagues worried that the Internet features would allow fans to watch blacked out games by streaming them at a slight time delay from other cities where the leagues had permitted the game to broadcast.

From a consumer perspective, the sports agency filings clearly demonstrated the danger in broadening the flag from a protection against massive redistribution to a general regime for controlling all "unauthorized" access outside the home. The flag was designed to protect DTV from massive online sharing – not as a way to help sports stadiums attract fans, or protect any of the other myriad business models of particular broadcasters or other industries that involved television. Localization controls were clearly outside the scope of the FCC's flag ruling.

Capitulation by the Applicants

In their initial responses to the MPAA opposition, all four companies expressed their opposition to the localization requirement:

- ***Thomson,* et al.*:*** "The SmartRight Applicants note that activation of such stringent proximity controls is not required by the scope of redistribution described in the Commission's November 4, 2003 *Broadcast Flag Report and Order*. Moreover, these proximity controls constrain inherent competitive and pro-consumer advantages of SmartRight's authorized domain system."[7]

- ***Real:*** "RealNetworks also asserts that the MPAA's position that the Helix Device DRM system must provide for proximity limitations is outside the scope of these proceedings."[8]

- ***Microsoft:*** "[T]he Broadcast Flag rules do not require the specific types of location-based redistribution controls the MPAA is requesting."[9]

[7] Reply of Thomson, et al. to Opposition of MPAA et al. in Docket MB 04-59 (filed Apr. 16, 2004) at 3.
[8] Reply of Real to Opposition of MPAA et al. in Docket MB 04-65 (filed Apr. 16, 2004) at i.
[9] Microsoft Reply at 3.

- ***TiVo:*** "The MPAA Parties' 'proximity of redistribution' concerns delve into matters the Commission has expressly placed outside the scope of this proceeding."[10]

Despite their principled objections, however, these companies were faced with the prospect of an extended battle in front of the FCC and the risk of ultimate rejection if they chose to oppose the MPAA's broad interpretation of the flag rules. In the end, each of the companies, with the lone exception of TiVo, ultimately agreed to accede to the MPAA's demands on proximity controls rather than face a prolonged fight in front of the Commission.

The question remained, however, how one could effectively enforce localization of content without disabling networking features altogether. In May, the MPAA sent a memo to the companies that were applying for approval, giving its response to this question. The memo, included in the Appendix to this paper, set out specific technical controls that the Association would consider to be sufficiently effective means of localization. Specifically, the MPAA's proposal rested on monitoring and controlling two particular technical parameters that the MPAA viewed as sufficient proxies for whether transmissions remained on a local network – the "time-to-live" (TTL) and the "round-trip time" (RTT) of transmitted "packets" of data. Since these parameters correspond only roughly to measures of geographical distance, there is no clear cut-off for what values these parameters should be set at to achieve the goal of localization. However, the MPAA said that it considered a TTL of 3 milliseconds and a RTT of 7 milliseconds to be sufficient.

Following the MPAA's memo, Thomson, Real, and Microsoft each filed revisions of their proposals to the FCC, saying they would limit TTL to 3 and RTT to 7, exactly as MPAA had suggested. The desire to avoid opposition led the three companies to cede remarkably detailed control over design decisions. As shown in the Appendix below, Real and Thomson even took the language of their revised filing directly from the MPAA's memo.

After Thompson, Real, and Microsoft officially stipulated to including the design changes requested by the MPAA, the Association dropped its opposition the three submissions. The MPAA, along with the NFL and MLB, continued to oppose TiVo, the one applicant that refused to adopt localization controls and stuck by its proposal to allow secure Internet transmissions.

[10] Reply of TiVo to Opposition of MPAA et al. in Docket MB 04-63 (filed Apr. 16, 2004) at ii.

Given the intense pressure that was likely on Thompson, Microsoft, and Real, it is understandable that they gave in. If they had decided to pursue their networking features, they would have risked not being approved, and consequently being months or even years behind their competitors. Despite its reasonableness as a corporate decision under the circumstances, however, the capitulation of the companies limited the ability of consumers to engage in lawful innovative uses of content.

The blow was somewhat lessened by the Commission's decision in August 2004. The Commission not only approved TiVo, but also approved SmartRight without localization controls, despite Thomson's explicit statement that it no longer sought such approval. The Commission should be applauded for taking this dramatic and consumer-friendly step. The Real and Microsoft filings were approved as amended, with the localization controls requested by the MPAA.[11]

The Commission's decisions on TiVo and Smartright notwithstanding, the specificity with which a third party was able to influence the product designs of technology applicants is alarming. Consumers lost the opportunity to make legal uses of video content, and the companies' concessions helped create an artificial uniformity across the approved products and an unnecessary restraint on the marketplace in rights protection options.[12]

Lessons from the Approval Process

That the FCC's approval process could allow a third party to effectively write the design specs for the implementation of localization controls in several submitted technologies clearly raises the specter of, in the FCC's words, "one industry segment exercising a significant degree of control over decisions."[13] The uncertainty and subjectivity of the approval process gave rise to this situation. By making the specific concessions that content owners said would allay their concerns, the technology companies were able to eliminate any opposition to their products. In contrast, TiVo, which refused to add proximity controls to its proposed technology, faced opposition until the end. Indeed, MPAA continued to oppose TiVo's technology even after the FCC approved it, filing a Petition for Reconsideration asking the FCC to revoke the approval.

[11] It is largely unclear from the Commission decision why it approved SmartRight without localization controls but not the Microsoft or Real proposals. See footnote 19 below for a slightly more detailed discussion of this question in the context of the issue of "device limits."

[12] In addition to Microsoft and Real's technologies (for which versions without localization controls were not approved by the FCC) at least one other technology approved by the Commission (DTCP over IP, Docket 04-61) also uses a RTT limit of 7 and TTL of 3 in transmitted packets to enforce localization.

[13] Order/FNPRM ¶ 52.

The FCC's decision in favor of TiVo clarified that proximity controls were not necessary for approval and were outside the scope of the flag rules in force at the time. The Commission wrote that the desire of the MPAA and NFL to protect business models based on local markets were "irrelevant to our stated goal of preventing indiscriminate redistribution."[14] The Commission concluded, therefore, that it would not "impose proximity controls as an additional obligation where other reasonable constraints sufficiently limit the redistribution of content."[15]

Great uncertainty remained, however, about what would constitute "other reasonable constraints" in a given case, and the Commission provided no additional guidelines except to say that it would continue to make decisions "on a case-by-case basis."[16] Had the flag rule withstood judicial challenge, this would have posed significant questions about the acceptable limits for other innovators seeking to introduce new consumer electronics devices and products for using television on computers. For example, would a technology that enables a 30 second excerpt to be taken in unprotected form from a protected 30 minute broadcast have been allowed? Such excerpting, and transformative use of the resulting clips, has become a staple of online political commentary.[17] But unless technologies were developed to facilitate excerpting for digital television, a flag regime could frustrate the ability of the public to engage in such commentary.

If a flag regime effectively discouraged the development of such new features – because applicants learned they could grease the mechanisms of approval by acceding to demands of other industry sectors over particular design decisions – then the flag regime could significantly dampen innovation and limit consumer uses of DTV.

Recommendations for a Better Process

The FCC wrote in the Flag Order that it sought to "formulate an open, objective approval process that will foster innovation and marketplace competition." The

[14] FCC Order In the Matter of Digital Output Protection Technology and Recording Method Certifications, MB Docket Nos 04-55 et al. (released August 12, 2004) ("Certification Order") ¶ 72.

[15] Certification Order ¶ 72.

[16] Certification Order ¶ 73.

[17] See, e.g., the numerous political video and audio "remixes" from the 2004 presidential elections. For example, on the Democratic side, "Keeping America Scared," available at: http://geekt.org/gopconstrm.mov; "Hard Working George," available at: http://www.simsadler.com/; and on the Republican side, "The Ultimate John Kerry Ad," available at: http://johnkerryads.websiteanimal.com/; "Kerry on Iraq War Documentary," available at: mms://media4streamtoyou.com//gwb/iraq_256k.wmv. (All URLs last accessed Sept. 1, 2005.)

transparency of the agency's approval decisions was admirable; our ability to write this report is based on the record that the process produced. However, in other key areas of objectivity – even-handedness, timeliness, and oversight – the process fell short of the Commission's goal.

Below are the areas in which CDT believes the FCC's flawed flag process would need to be improved, if Congress were to decide to authorize the agency to implement the flag. We believe that any flag authorization legislation should carefully address each of these issues, rather than leaving open-ended discretion with the FCC. (CDT's full list of recommendations for potential flag legislation, covering not just these process-related matters but also the treatment of public affairs content and notice to consumers about interoperability limitations, is set forth in a separate paper, "Broadcast Flag Authorization Legislation: Key Considerations for Congress.")

OBJECTIVITY – The more uncertainty and discretion there are in the standards for approval, the greater the pressure will be on companies to make concessions in their products to eliminate any objections, and the greater will be the ability of third parties to exercise an effective veto over a new technology.

The "interim" approval process the FCC employed was based on a non-exhaustive list of factors that the Commission said it might (though was not required to) consider. These general guidelines included "technological factors," "applicable licensing terms," and "the extent to which the [technology] accommodates consumers' use and enjoyment" of broadcast content. In addition, the FCC reserved the right to consider "any other relevant factors the Commission determines warrant consideration."[18]

Such a wide-open set of criteria permits too much discretion. In contrast, CDT has advocated that, if there is to be a flag regime, the approval of compliant technologies hinge on one main functional requirement, articulating the narrow stated purpose of the flag:

> *Does the technology effectively frustrate an ordinary user from indiscriminate redistribution of protected content to the public over the Internet or through similar means?*

In CDT's view, this should be the sole or dominant standard for approval of a copy protection technology. In addition, any future broadcast flag rules should explicitly indicate some of the uses that will be authorized if implemented consistent with the protection criterion. For example, the rules should explicitly

[18] Order/FNPRM, Appendix B at 45.

indicate that secure redistribution to a small number of other devices over the Internet will be permissible[19] and that excerpting will be allowed.

No rules could exhaustively specify with certainty the decision that would be made on every future technology, because technological innovation necessarily creates possibilities that cannot be anticipated. Nonetheless, a carefully structured approval process could do far more to reduce uncertainty and subjectivity than the initial interim process conducted by the FCC.

BURDEN OF PROOF ON THE OPPOSITION – The FCC's process included no explicit statement of where the burden of proof lay – or what it was – in approval decisions. Any revived flag regime must fix this deficiency. Specifically, in order to achieve the FCC's stated goal of facilitating a diverse marketplace, the presumption must always be in favor of approval of technologies that meet the low threshold of proving *prima facia* compliance with the purpose of the flag. Those who would try to prevent the entry of a product into the marketplace must have the burden to prove a substantial likelihood that it will result in indiscriminate redistribution.

Various forms of "self-certification" were proposed by commenters in the FCC's flag proceeding, as a way to institutionalize the presumption we recommend. Regardless of the particular scheme, the clarification of burdens would help embolden product makers and limit the leverage of third parties seeking to block new technologies from the marketplace.

NO PARALLEL PATHS – Several stakeholders had suggested that the Commission should adopt two parallel approval processes. The first option would be something like the FCC's interim process, in which a determination would be made by the Commission itself. The second option would be on a model originally proposed by the content companies, under which a device could be approved if a sufficient number of studios or broadcast groups signed off on it.

The experience with the FCC's approval decisions indicates why a parallel process approach is dangerous for consumers and innovation. As CDT wrote in

[19] The FCC's approval of TiVo and SmartRight, even if it were given some weight as precedent in a new, legislatively authorized flag regime, would not be sufficient to assure developers that transmission over the Internet will be permitted if the number of devices that can receive the transmission is limited. The Commission declined to take the same steps for the Microsoft and Real proposals that it did for SmartRight (i.e., approving the versions of the proposals without proximity controls despite the companies' concessions) despite recognizing that Real and Microsoft "also utilize device limits as part of their system." Certification Order at 34 n.322. The Commission cited "affinity based parameters" of TiVo and SmartRight as reasons for this distinction. Certification Order ¶¶ 72-73). This murky precedent would leave developers without clear guidelines on what is permitted. As noted above, the Commission had said that it would continue to make determinations "on a case-by-case basis," hardly reassuring to advocates and developers looking for certainty and objectivity.

comments to the FCC, "[c]reating multiple approval avenues would effectively place different standards on technologies that had the 'blessing' of established market players than on novel technologies striving for market acceptance . . . In addition, a "parallel tracks" approach could eliminate transparency in a subset of approval determinations. No proposed technology should be exempted from [an] open and publicly accountable process."[20]

It is instructive to consider what could have happened had a parallel approvals approach been in place for the initial round of approval decisions. Of the thirteen technologies seeking approval, *TiVo could have been the only application considered under the Commission's open, public process.* Of the thirteen, nine would probably have been approved almost immediately – these were unopposed by the MPAA's coalition and therefore would likely have garnered the approval of the requisite number of major studios. For the three that eventually adopted proximity controls – Microsoft, Real, and Thomson – the nine immediate approvals would have greatly increased the incentive to make concessions even sooner, in order to avoid giving their competitors a first mover advantage. In any case, the MPAA announced its approval of these additional three technologies as of June 21, 2004, once they capitulated on the localization issue.[21] At this point, TiVo would likely have been the only technology still seeking the approval of the Commission. This could have given TiVo's competitors a month and a half head-start before TiVo was approved by the Commission on August 4th. Under these circumstances, it is reasonable to ask: Would TiVo have continued to press its application without concession? Would the Commission's process have reached the same conclusion? And would consumers have had the same public record on which to base critical examinations of the process?

In short, no small set of established players should be given regulatory authority over DTV devices. This would discourage innovation, eliminate transparency and accountability for many decisions, and compromise the commendable goals laid out by the Commission for the flag process.

TIMELY DECISION-MAKING – As suggested above, a critical problem for any flag regime is the expedited decision-making needed if the flag is not to become a roadblock to innovation in quickly moving product cycles. Possible delays at the Commission must not become a motivation for making concessions.

The FCC's interim process featured no specific guarantee of how long review of submitted applications would take. Such an indefinite timescale strongly

[20] Reply Comments of Center for Democracy and Technology, MB Docket 02-230 (filed March 15, 2004) at 9.
[21] See "Broadcast Flag Proximity Control Talking Points," MPAA *ex parte* filing, MB Docket 04-63 (filed July 21, 2004).

encourages applicants to come to the FCC with any potential obstacles to approval already smoothed over. Any future process must provide stronger assurances to applicants. It should guarantee that all approval decisions will be made within a reasonably short period of time, specified exactly in the rules.

OVERSIGHT – The FCC proceedings clearly demonstrated the dangers in the broad regulatory regime created by the flag. A robust oversight mechanism would be needed to ensure that a future flag process does not get out of hand. In our comments to the FCC on the Flag Order, CDT called for the creation of an oversight advisory board made up of individuals from diverse industry and public interest backgrounds. Such a board should include representatives of consumer and public interest groups, content producers, manufacturers, and technology companies. A board of this kind would provide an independent consumer voice that was absent from the Commission's initial flag process.

If a flag regime is adopted, this oversight board should report on the status of the flag system's implementation no less frequently than once per year. It should be within the board's mandate to recommend that the flag system be substantially changed, or even discontinued. The board should also have the task of considering whether criteria for content protection technology certification should be changed or removed.

Conclusion

When the FCC adopted the broadcast flag rules, it gave itself a very difficult job. Despite its admirable efforts to keep the focus of the flag regime relatively narrow, the rules still put the Commission in a position of exceptional power in approving or denying the offerings of consumer electronics companies and software vendors. The Commission created a process that would have made the agency the gatekeeper to the market in devices that handle DTV content.

Recognizing this, the Commission sought to achieve balance in the flag rule and stated its intent to ensure that the flag regime would not stymie innovation or hold back the DTV transition. The FCC should be applauded for emphasizing the narrow goals of the flag and asserting its intent to promote Internet technologies in its initial round of approvals.

Nonetheless, the FCC's scheme was marked by some serious problems. From the outset, critics of the flag underscored the danger of creating a regulatory regime for design decisions in rapidly evolving digital technologies. The history of the initial flag regime gives credence to concerns about limiting the lawful flow of information and hobbling innovation in computers and on the Internet.

For any future flag regime to avoid these pitfalls, the approval process for technologies must be expedient, open, and predictable, without preferential treatment for particular industries, and with robust oversight. These requirements should be fully reflected in any legislation to authorize the FCC to proceed with implementing a broadcast flag regime.

CDT looks forward to working with Congress and other interested parties if and when broadcast flag authorization legislation is considered on Capitol Hill.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact:
Jerry Berman, President
David Sohn, Staff Counsel
http://www.cdt.org

Appendix

MPAA Memo to Companies Applying for Approval (May 19, 2004)	**RealNetworks Letter to FCC on Revisions to Its Filing (July 1, 2004)** *(Language adopted directly from MPAA in **bold**)*
"Local Proximity Content Control - An authorized Broadcast Flag content protection technology must incorporate local proximity content control mechanisms that provide affirmative and reasonable constraints on controlling the digital redistribution of Unscreened and Marked Content through the digital outputs and connections of a Covered Demodulator Product or a Downstream Covered Product beyond the home or other similar local network environment of such Covered Product.	"RealNetworks also provides additional information to the Commission on the dialogue between the MPAA parties and RealNetworks concerning matters of content protection and local proximity limitations. One critical result of these discussions is agreement on the specific parameters defining Helix DRM's initial proximity content controls. RealNetworks and MPAA have agreed on the following initial proximity content control mechanisms and parameters to be applied to RealNetworks' interim certification.
At a minimum, local proximity detection requires:(i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of Marked or Unscreened Content output from a Covered Product source device; (ii) confirmation that any Internet Protocol (IP) packets of Marked or Unscreened Content received by a Covered Product sink device have an IP Time to Live (TTL) parameter value of no greater than 3; and (iii) confirmation by the Covered Product source device for any transmission of Marked or Unscreened Content (including over point-to-point wired connections) that one secure, valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the Covered Product sink device prior to completing the sink device's authentication request. Time to Live (TTL) is defined in Internet Standard RFC 791 STD 5.	**At a minimum,** Helix's DRM **proximity detection will include: (i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of** Helix DRM **protected Marked Content output from a** Trusted Recorder**; (ii) confirmation that any IP packets of** Helix DRM **protected Marked Content received by a** Trusted Client **have an IP TTL parameter value of no greater than 3; and (iii) confirmation by the** Trusted Recorder **for any transmission of** Helix DRM **protected Marked Content (including over point-to-point wired connections) that one valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the** Trusted Client **prior to completing the** Trusted Client's **authentication request. Time to Live (TTL) is defined in Internet Standard RFC 791 STD 5.**
The measurement of Round Trip Time (RTT) by a Covered Product source device must occur: (a) after power-up of the Covered Product source device when an active Covered Product sink device requests authentication; (b) when the last transmission of content-based packet traffic between a Covered Product source device and sink device has occurred more than 120 minutes prior; and (c) when the last successful RTT measurement of 7 milliseconds or less between a Covered Product source and sink device has occurred more than 24 hours prior.	**The measurement of Round Trip Time (RTT) by a** Trusted Recorder will **occur: (a) after power-up of the** Trusted Recorder **when an active Trusted Client requests authentication; (b) when the last transmission of content-based packet traffic between a** Trusted Recorder **and a** Trusted Client **has occurred more than 120 minutes prior; and (c) when the last successful RTT measurement of 7 milliseconds or less between a Trusted Recorder and a** Trusted Client **has occurred more than 24 hours prior.**
The determination of RTT must be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating Covered Product sink device receiving the protected content can respond to the RTT measurement message. A Covered Product source device may attempt the measurement of RTT multiple times until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus the RTT measurement is the minimum RTT value measured and not the average of all RTT values measured."	**The determination of RTT** will **be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating** Trusted Client **receiving the** Helix DRM **protected content can respond to the RTT measurement message. A** Trusted Recorder **will attempt the measurement of RTT until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus the RTT measurement** will **be the minimum RTT value measured and not the average of all RTT values measured."**

MPAA Memo to Companies Applying for Approval (May 19, 2004)	**Thomson/MPAA Joint Letter on Revisions to Filing (May 28, 2004)** *(Language adopted directly from MPAA in **bold**)*
"Local Proximity Content Control - An authorized Broadcast Flag content protection technology must incorporate local proximity content control mechanisms that provide affirmative and reasonable constraints on controlling the digital redistribution of Unscreened and Marked Content through the digital outputs and connections of a Covered Demodulator Product or a Downstream Covered Product beyond the home or other similar local network environment of such Covered Product.	"Thomson and MPAA also have engaged in a productive dialogue following the April 16th submission. One critical result of these discussions is agreement on the specific parameters defining SmartRight's initial proximity content controls. Specifically, SmartRight Applicants and MPAA have jointly agreed on the following initial proximity content control mechanisms and parameters.
At a minimum, local proximity detection requires:(i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of Marked or Unscreened Content output from a Covered Product source device; (ii) confirmation that any Internet Protocol (IP) packets of Marked or Unscreened Content received by a Covered Product sink device have an IP Time to Live (TTL) parameter value of no greater than 3; and (iii) confirmation by the Covered Product source device for any transmission of Marked or Unscreened Content (including over point-to-point wired connections) that one secure, valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the Covered Product sink device prior to completing the sink device's authentication request. Time to Live (TTL) is defined in Internet Standard RFC 791 STD 5.	**At a minimum,** SmartRight **local proximity detection will include:(i) setting the Internet Protocol (IP) packet header parameter Time to Live (TTL) to 3 in all transmitted IP packets of Marked or Unscreened Content output from a Covered Product source device; (ii) confirmation that any Internet Protocol (IP) packets of Marked or Unscreened Content received by a Covered Product sink device have an IP Time to Live (TTL) parameter value of no greater than 3; and (iii) confirmation by the Covered Product source device for any transmission of Marked or UnscreenedContent (including over point-to-point wired connections) that one valid measurement of a Round Trip Time (RTT) of 7 milliseconds or less has been made between itself and the Covered Product sink device prior to completing the sink device's authentication request. Time to Live (TTL) is defined in Internet Standard RFC 791 STD 5.**
The measurement of Round Trip Time (RTT) by a Covered Product source device must occur: (a) after power-up of the Covered Product source device when an active Covered Product sink device requests authentication; (b) when the last transmission of content-based packet traffic between a Covered Product source device and sink device has occurred more than 120 minutes prior; and (c) when the last successful RTT measurement of 7 milliseconds or less between a Covered Product source and sink device has occurred more than 24 hours prior.	**The measurement of Round Trip time (RTT) by a Covered Product source device** will **occur: (a) after power-up of the Covered Product source device when an active Covered Product sink device requests authentication; (b) when the last transmission of content-based packet traffic between a Covered Product source device and sink device has occurred more than 120 minutes prior; and (c)when the last successful RTT measurement of 7 milliseconds or less between a Covered Product source and sink device has occurred more than 24 hours prior.**
The determination of RTT must be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating Covered Product sink device receiving the protected content can respond to the RTT measurement message. A Covered Product source device may attempt the measurement of RTT multiple times until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus the RTT measurement is the minimum RTT value measured and not the average of all RTT values measured."	**The determination of RTT** will **be measured using a cryptographically secure protocol to prevent any form of spoofing and to ensure that only the authenticating Covered Product sink device receiving the protected content can respond to the RTT measurement message. A Covered Product source device will attempt the measurement of RTT until it achieves a single valid measurement of 7 or fewer milliseconds or determines that this requirement cannot be met and completion of authentication is halted. Thus, the RTT measurement** will be **the minimum RTT value measured and not the average of all RTT values measured."**