

General Counsel
Copyright GC/I&R
PO Box 70400
Southwest Station
Washington, DC 20024-0400

Reply Comment of:
Matthew Perkins¹
Minneapolis, Minnesota

For United States Copyright Office Rulemaking on: Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (2006).

List of Initial Comments, to which this Reply Comment is responsive:

Comment 12 (Matthew Ford)

Comment 17 (Christopher Meacham)

Comment 22 (Gabriel Ferreira)

Comment 27 (Floyd Nash)

Comment 44 (Dennis Starker)

Comment 45 (Alan Rouse)

Comment 46 (Trey Williams)

Comment 48 (Brent Dolphin)

Comment 52 (John Morton)

Comment 56 (Ron and Mattie Wackwitz)

Comment 59 (John E. Gilmore Jr.)

Comment 61 (Christopher Peters)

Proposed Class:

Audiovisual works conveyed through digital, terrestrial radio broadcast, which are intended for free, over-the-air access by all persons within the range of the broadcast (i.e., "Broadcast Flag").

¹ The submitter is a systems analyst, not a lawyer. It is hoped that the reader will forgive all non-lawyerly deficiencies.

Summary of Argument:

The 74 Initial Comments for the present Rulemaking appeared on the Web site of the United States Copyright Office with an unusual disclaimer, apparently dismissing a number of Initial Comments for a variety of reasons. One reason was that certain Initial Comments “have not identified an access control that would implicate the prohibition of circumvention;” and it was implied that a Reply Comment would not be considered unless it responds to a “genuine proposal.”

At least 12 Initial Comments, referenced above, complain of the “broadcast flag” system for marking digital television to enable downstream copy- and distribution-control measures. Basic knowledge of the broadcast flag, and common sense, do in fact seem to suggest that the measure does not “control access.”

However, that view cannot rule the measure outside of 1201(a): the statutory language itself, and prevailing views on that language, must control. In this Reply Comment, I attempt to illustrate, by factual and textual analysis, that the customary interpretations of 1201(a) force the conclusion that a broadcast flag system, which all must agree “controls access” to nothing at all, nevertheless must be covered by 1201(a) if disruption of settled views is to be avoided, and if adherence to the statutory text is to be achieved.

I do not offer any firsthand, factual evidence of any difficulty with respect to the broadcast flag measure, and I remain silent on what harms, if any, do or would result from the 1201(a) prohibition with respect to that measure. The Register should conduct those inquiries based on the evidence presented. The Register should not, however, begin those inquiries without first determining whether the broadcast flag system is, in fact, a 1201(a) measure. And, while the Register may find at this preliminary stage that a 1201(a) exemption for the broadcast flag system is not a “genuine proposal,” it is urged that the analysis below be considered prior to making that determination.

Argument:

I. The Intent of “Broadcast Flag” Comments Should Be Restated As a “Class of Works” Which The Register May Consider Recommending for Exemption.

Several commenters make reference to the “broadcast flag” requirement, a now-extinguished mandate from the FCC that all digital television (DTV) receiving devices recognize, preserve, and adhere to, an instruction which may be embedded within a DTV transmission and which dictates quantitative or qualitative limits on reproduction or distribution of DTV content. It is appropriate, at the outset, that the commenters’ intent be stated as a “class of works” which the Register may consider in the present rulemaking. I would suggest the following: ***Audiovisual works conveyed through digital, terrestrial radio broadcast, which are intended for free, over-the-air access by all persons within the range of the broadcast.*** This proposed class is far narrower than the simple category of “audiovisual works.” It limits that category in three important respects: it confines the class to works delivered over terrestrial digital television signals; it requires that no payment or obligation be placed upon an individual citizen as a condition of access (“free”); and it requires that a covered work be one whose distribution indiscriminately flows to all persons in the practical range of the broadcast (“within the range”). These three limitations restrict the scope of the class itself, and do not refer in any manner to the users, or expected uses, of works among the class. Finally, the “conveyed” clause is intended to exclude from the class any alternative method for acquiring terrestrial DTV broadcasts, so that DTV content delivered over cable and satellite systems would retain full protection of 1201(a).

II. Broadcast Flag Recognition, Preservation, and Compliance Is a Process Required to Gain Access to Digital Television Content.

1. Under Existing Law, the Broadcast Flag’s Function to Restrict Copying or Distribution Cannot Foreclose its 1201(a) Protection.

It would be disingenuous to conclude, without further discussion, that the broadcast flag system is “obviously” a measure which restricts copying or distribution, not access, and therefore falls categorically beyond the scope of the present rulemaking. The matter is not so obvious.²

The CSS system used on DVD Video discs is, likewise, a mechanism for prevention of copying and distribution; and yet, while not relying on 1201(b) for its ultimate injunction, *Reimerders* and

² 2003 Register’s Recommendation, at 45: “It therefore appears that the primary purpose of a protection system does not necessarily determine whether it is an access control, or a copy control, or both.”

Corley both suggested that 1201(b) could provide an alternate basis.³ *Davidson* stands for a comparable duality; that is, a 1201(a) remote authentication system can function as a 1201(b) measure by inhibiting the usefulness of unauthorized copies.⁴ And *321 Studios* explicitly favors the notion that a single measure can be categorized under both 1201(a) and 1201(b).⁵ The fact that many technological measures are commonly believed to find protection under both 1201(a) and 1201(b) requires that the inapplicability of 1201(a) to a broadcast flag system cannot be presumed simply because 1201(b) also applies. If it is accepted that *both* may apply, then the capacity for a measure to restrict copying cannot, by itself, exclude the measure from 1201(a).

Of course, the differential treatment by Congress for access-control measures in 1201(a), and copy-control measures in 1201(b), suggests very strongly that it was the intent of Congress that the two categories of measure be treated separately, and therefore that the categories are, in fact, distinct. That the statute is construed in defiance of such an obvious duality may suggest that the prevailing state of 1201(a) interpretation is deeply and fundamentally flawed. But at this early point in the analysis, it should suffice that the broadcast flag system cannot, without further discussion, be excluded from 1201(a) on the basis of its intended purpose.

2. To “Gain Access to” DTV Programming is to Perform a Broadcasted Audiovisual Work.

³ *Reimerdes* at 30, fn. 133 (“Plaintiffs rely also on Section 1201(b), which is very similar to Section 1201(a)(2) except that the former applies to trafficking in means of circumventing protection offered by a technological measure that effectively protects “a right of a copyright owner in a work or a portion thereof” whereas the latter applies to trafficking in means of circumventing measures controlling access to a work.”); and fns. 154, 157 (“[1201(g)] is a defense only to claims under Section 1201(a)(2), not those under Section 1201(b)... 1201(j) provides no defense to a Section 1201(b) claim.”).

⁴ *Davidson* at 32 (“The bnetd emulator developed by the defendants always allows the Blizzard game to access Battle.net mode features even if the user does not have a valid or unique CD Key.... Unauthorized copies of the Blizzard games were played on bnetd servers.”) A user lacking a valid or unique CD key is presumably a user in possession of an unauthorized copy.

⁵ At 15: “Accordingly, this Court finds that 321’s software is in violation of both § 1201 (a)(2) and § 1201 (b)(1), because it is both primarily designed and produced to circumvent CSS, and marketed to the public for use in circumventing CSS.”

To qualify for 1201(a) protection, a measure must, "in the ordinary course of its operation, require[] the application of information, or a process, or a treatment, with the authority of the copyright owner, to gain access to a work." It is tempting to conclude that a broadcast flag system does not require any process as a condition of gaining access: it only restricts activities subsequent to the act of accessing. At least one flawed premise informing this conclusion is a misuse of "to gain access to a work" to mean only the precise act of acquiring that work.

In reality, "to gain access to a work" should be understood as carrying two different meanings, depending on the measure in place. Consider two standard access-control measures, both of which squarely intersect with common experience at the time of the 1998 passage of the DMCA: a subscription web site, and digital satellite programming. Charted below are the steps an ordinary user would follow to "gain access to a work" using either of those systems.

| Productive (web site) | Interactive (digital satellite) |
|----------------------------------|--|
| 1. Gain Authority | 1. Gain Work |
| 2. Gain Means | 2. Gain Authority |
| 3. Use Means | 3. Gain Means |
| 4. Gain Work | 4. Use Means |

The web site example, such as New York Times Online which requires user registration to acquire an article, will be considered a Productive measure: the measure is literally the mechanism which produces a copy or transmission of the work for a particular user.⁶ A person subscribes to the service ("gain authority," used here to mean authority to access the work); acquires a set of login credentials, such as an ID/password combination ("gain means"); submits those credentials into a login system ("use means"); and finally, upon recognition by the login system that the user-supplied credentials are valid, receives a copy or transmission of the desired work ("gain work").

Digital satellite programming functions with a significantly different set of operations and purposes. Acquisition of the work ("gain work") is the default condition, since the satellite signal is indiscriminately blasted into the cells of every living thing on the continent at all times. Perceiving that signal is as simple as pointing a quasi-parabolic object in the right direction and

⁶ In this Reply Comment the word "copy" (noun) is intended to include both copies and phonorecords, as the distinction between the two is not directly relevant to the topic.

connecting it to some knickknacks from Radio Shack. The technological measure used to distinguish between subscribers and non-subscribers is to encrypt the transmission, and provide an interoperative key or token only to subscribers. Unlike Productive measures, this category serves not to choose who will acquire the signal, but rather to choose who will interact with that signal to produce an audiovisual performance. I refer to this category as Interactive. The ordinary course of operating this measure is to subscribe with the service provider (“gain authority,” in this case to access the work); receive a key or token for decrypting or descrambling (“gain means”); and apply the key or token to the signal (“use means”) ultimately to produce an audiovisual performance.

Of the two access-control categories, Productive and Interactive, the most diverse and sophisticated among the market for copyrighted works seems to be Interactive. Numerous technological measures are designed not to facilitate the act of acquiring a copy or transmission, but rather to interact with an already-present copy or transmission. One noteworthy, non-encryptive example of this category is free-trial software, which may be downloaded and used for a limited time (“Gain work”) but which self-deactivates after a trial window. Subsequent program execution requires a person to buy a license (“Gain Authority”) bundled with an activation code (“Gain Means”) for conveyance into the program (“Use Means”). Such a measure does not produce the copy, which already exists on the person’s computer. Rather, it interacts with that copy to result in program execution at the user’s whim.

Viewed in light of these two access-control categories, it is clear that the act of “gain[ing] access to a work” has not one meaning, but two. For Productive measures, “to gain access to a work” is to acquire a copy or transmission of the work. For Interactive measures, “to gain access to a work” is to generate from a copy or transmission the intended user experience; for example, to render a performance or display (for works generally, such as literary works, audiovisual works, sound recordings, etc.), or to execute (for computer programs).

Plainly, a broadcast flag system does not result in the acquisition of DTV programming. But that fact alone cannot render the system unprotected under 1201(a), unless all other Interactive measures are likewise unprotected. The appropriate condition, therefore, for determining whether the process of flag compliance is required “to gain access” to DTV programming is whether it is required *to perform the broadcasted audiovisual work*.

3. A Technological Measure That “Effectively Controls Access” is Construed to Require an “Authorized Process.”

The statute defines a 1201(a) measure in these words: “A technological measure ‘effectively controls access’ if, in the ordinary course of its operation, it requires the application of information, or a process, or a treatment, with the authority of the copyright owner, to gain access to a work.” Within this gem of legislative opacity rests a remarkably positioned phrase, “with the authority of the copyright owner,” which may be interpreted coherently in at least two mutually incompatible ways. It may serve to identify, or alternatively to qualify, that which is “required.” If read to identify, then the definition could be restated as follows:

A technological measure ‘effectively controls access’ if, in the ordinary course of its operation, it requires [a process] to gain access to a work, **and also requires the authority of the copyright owner** to gain access to a work.

Alternatively, if read to qualify, the definition means this:

A technological measure ‘effectively controls access’ if, in the ordinary course of its operation, it requires [a process] **which is performed with the authority of the copyright owner**, to gain access to a work.

In other words: either a process and authority are required, or an authorized process is required. The two meanings could hardly be more different. The identifying reading (“and”) anticipates a measure which accomplishes two tasks: it incorporates a process necessary for the act of gaining access; and it depends on a specific knowledge that the copyright owner has granted authority to access a work.⁷ The qualifying reading (“authorized process”) anticipates the first task, incorporating a process, and further requires that such process is authorized to occur; but the second task, that of dependence on authority to access, is not present and, one must presume, irrelevant.

⁷ I include “specific knowledge” here because a “technological measure,” like any set of systematic or logical operations, cannot “require the authority of the copyright owner” unless it receives or depends upon some information which represents, to the measure, an assertion of that authority. This is a different conditional set than that of a technology whose legal status is either “authorized” or not, by a copyright owner.

To recognize the breadth of difference between the two interpretations, identifying and qualifying, it is helpful to note a condition of Interactive measures which I describe as “transactional independence” between the work, and authority to access the work. Encrypted satellite TV and activation-dependent software share a condition of transactional independence. A person first acquires a copy or transmission of the work; subsequently and separately, the person acquires a means (whether a decryption key, an activation code, or something else), which implies, and which represents, authority to access. The important point is that, for a work incorporated within a typical Interactive measure, acquisition of the copy or transmission does not result in authority to access: that authority is obtained by an independent transaction. The obvious alternative to transactional independence is all works for which lawful possession, and nothing else, implies authority to access.

(The precise strategy employed by a copyright owner to extract value will, of necessity, have some bearing on whether transactional independence exists. A business model extracting value only from the “work” and not from the means (such as conventional DVD Video) suggests a lack of transactionally-independent “authority to access.” Alternatively, a copyright owner may give away the work at reduced or zero cost, while extracting some, or all, value from a transaction conveying the means. This latter model suggests transactional independence. Physical media does not confine the copyright owner’s choice: a transactionally-independent DVD model can be imagined, where a copyright owner distributes free or low-priced discs but with payment required for the decryption key.⁸ Importantly, if the copyright holder extracts no value from the transaction conveying the means, then avoiding or bypassing that mechanism presents no loss of value to the copyright owner. Since 1201(a) may be invoked only by a person “injured,” one should expect that the only conceivable 1201(a) claimant under such a revenue model should be the entity denied value by the avoidance – in the case of encrypted DVDs, that party is DVD-CCA.⁹)

⁸ This very model was actually explored briefly in the late 1990s, for a pay-per-view DVD alternative called DIVX.

⁹ The reader is invited to ponder the legal meltdown resulting from a statute which confers standing to DVD-CCA, but which unilaterally empowers a third party to negate the claim (“to circumvent” is “to decrypt ... without the authority of the copyright owner”).

The idea of transactional independence is directly relevant to which interpretation, identifying or qualifying, controls the “authority” phrase, above. If one accepts that an Interactive measure requires satisfaction of “authority to access” (the identifying interpretation), then transactional independence is a necessary condition. This is because, without transactional independence, the work would, at all times and for all possessors, implicitly convey “authority to access” by nothing more than the work’s very existence. With respect to authority, the measure would have nothing to require.¹⁰ Alternatively, if one accepts that a measure requires only an authorized process (the qualifying interpretation), there is no need for transactional independence: whether authority to access is implied or not, access may be obtained only by operating the authorized process.

The identifying interpretation (a process “and” authority are required) is fully consistent with both access-control categories defined above, Productive and Interactive. Each example Interactive measure, satellite TV encryption and software activation, operates upon a work with, not insignificantly, transactionally-independent authority to access. The qualifying interpretation (“authorized process” is required), however, under which transactional independence is irrelevant, is so very different in nature from the Productive and Interactive categories that it requires an entirely new category to accommodate it.

| Productive (web site) | Interactive, TI (digital satellite) | Interactive, NTI (DVD encryption) |
|----------------------------------|--|--|
| 1. Gain Authority | 1. Gain Work | 1. Gain Work |
| 2. Gain Means | 2. Gain Authority | 2. Use Authorized Means |
| 3. Use Means | 3. Gain Means | |
| 4. Gain Work | 4. Use Means | |

This new category, Interactive/NTI, consists of all measures protecting a work which lacks transactionally-independent authority to access. DVD encryption fits into this new category. It is uncontested that DVDs are not transactionally independent: a DVD, and “authority to access” the DVD’s content, are conveyed by the same transaction. The only method by which DVD encryption may be covered under 1201(a) is under the qualifying interpretation, where the

¹⁰ Put more simply: if the physical fact of a copy or transmission is enough to satisfy a measure’s required “authority to access,” then for an Interactive measure – which, by definition, operates upon an existing copy or transmission – that requirement would always be met. The entire “requires authority to access” phrase would be effectively excised from the statute.

measure requires an authorized process. For the same reasons, a variety of other measures protecting not-transactionally independent works gain 1201(a) protection only by employing the qualifying interpretation: dongle-dependent software; copy-resistant CD Audio; DVD Region Coding; etc.

Under the identifying interpretation, the broadcast flag system could not be a 1201(a) measure. DTV and “authority to access” DTV are not transactionally independent, and so the broadcast flag system cannot “require authority to access” DTV programming. But the same interpretation also excludes from 1201(a) all other not-transactionally independent measures described above.¹¹ In addition, reconsideration would be in order for the prevailing view that a single measure can be “merged” for protection under both 1201(a) and 1201(b). Every such measure “requires [a process]” to perform, display or execute, and therefore snuggles comfortably into the language of 1201(a); but every such measure also lacks transactionally-independent “authority to access.” Under the identifying interpretation, which demands transactional independence, one is forced to conclude that a “merged” measure can only function to restrict copying.¹² While it may be questioned whether the identifying interpretation reflects either Congressional intent or sound

¹¹ The conclusion that these measures might lie beyond the reach of 1201(a) is one which need not offend common sense. DVD encryption and dongles exist only to prevent copying. And Region Coding’s presumptive purpose, isolating distribution within nations and continents, reflects a measure protecting the distribution right (importing, exporting); trans-regional incompatibility for a given traveler is certainly an externality, but it is not the measure’s objective. Note also, this revolutionary notion that 1201(a) implies a condition of transactional independence would only marginally disrupt these measures’ DMCA protection: a reasonable person could properly classify each measure under 1201(b).

¹² There are two reasons for this. First, a lack of transactionally-independent “authority to access” means that the work, and authority to access, are both present. And second, it follows that if a person is authorized to access a work, then the only conceivable purpose for a limitation on the means of performance, display or execution can be to confine such acts in a manner intended to prevent copying and redistribution.

One might imagine that a second purpose for controlled performance or execution is “tethering,” or locking a user into a specific architecture to discourage migration to competing architectures. Apple’s iTunes Music Store and iPod, collectively, are one noteworthy example. This purpose is merely a corollary to the purpose of copy-prevention: permissive copying enables architectural portability. That condition negates the market strategy of lock-in, so the act of copying is, as a strategic matter, intended to be restrictive.

policy, there can be no doubt that it results in a statute that is far more coherent and less subjective than under the alternative qualifying interpretation.

But in the end, whether out of deference to the judiciary or out of fidelity to prior recommendations, the Register must endorse the qualifying interpretation. Under that reading, 1201(a) must cover the broadcast flag system if that measure “requires” flag compliance, and if flag compliance is an “authorized process.”

4. The Broadcast Flag “Requires” the Process of Recognition, Preservation, and Adherence.

The determination of whether the broadcast flag system “requires” compliance must begin with common sense. If all DTV devices are flag-compliant by Federal mandate, then one cannot access DTV programming without performing the flag-compliance process (recognition, preservation, adherence). But even absent a mandate, the prevalence of flag-compliant DTV devices, along with a likely resistance by manufacturers to identify their devices as either compliant or not, may limit consumer choice so completely that compliance is a *de facto* requirement.¹³ Fortunately, finding the answer to whether flag compliance is “required” need not involve speculation upon a series of unknowables, such as whether a Federal mandate is “more likely than not” in the coming three-year period, or what hypothetical fraction of DTV devices will be flag-compliant in 2009. One needs only to consider a single person, using a flag-compliant device to receive a flagged DTV transmission. That condition is absolutely certain to exist today, and it requires no guesswork. So the question becomes: for this person, using a flag-compliant DTV device to receive a flagged DTV transmission, does the broadcast flag system “require” flag-compliance to perform DTV programming?

The question is deceptively complex. The pat answers above, relying on design mandates and market share, satisfy very superficially; but without further exploration they are inadequate and too vulnerable to common-sense objections. I will attempt to anticipate and deconstruct the most predictable, intuitive, and facially appealing arguments that flag compliance is not, in fact, “required.”

¹³ One source of “resistance” implicit here is that, under the Supreme Court’s holding in *Grokster*, the marketing of flag-noncompliance in a DTV device invites a cognizable inducement claim.

A. “Requires” cannot imply absolute necessity.

In one sense, “requires” may imply an absolute dependence. One may argue that the broadcast flag system does not require a process (recognition, preservation, adherence) to perform DTV programming, and so the broadcast flag system is not a 1201(a) measure. This argument states the simple fact that performance of DTV content may be achieved independently of whether flag recognition/preservation/adherence takes place, and concludes that 1201(a) cannot apply. To the extent that this argument conditions 1201(a) protection on the difficulty of avoiding or bypassing the measure, it is flawed.

Specifically, the argument selectively imposes a higher burden of operational constraint for the measure under discussion. For purposes of separating constraints, I will use the term “Practical” to describe a constraint involving absolute impossibility. Encryption, for example, is a Practical constraint on an audiovisual work because an audiovisual performance is physically impossible without first reversing the encryptive operation.¹⁴ An “Artificial” constraint is everything else: that is, constraints which are “required” only in the sense that they depend upon a sequence of operations and conditions, not all of which are absolutely necessary. The defining trait of Artificial constraints is susceptibility to avoidance or bypassing (in a hypothetical sense, at least), since they are not absolute barriers to access. Other than encryption, virtually all mechanisms presently understood as access-control measures depend on Artificial constraints and, it follows, bear the characteristic vulnerabilities incumbent in such constraints: a login system may be bypassed; an activation code may be forged or spoofed; dongle-dependent software may be modified; etc.

To deny 1201(a) protection to a broadcast flag system for that measure’s inefficacy holds the broadcast flag system to a higher standard than demanded of access control measures in general: the broadcast flag is expected to impose a Practical constraint upon access, while other measures may impose only an Artificial constraint. DVD Region Coding, previously concluded by

¹⁴ The relative difficulty of decryption is irrelevant to this categorization. So, whether a skilled person may decrypt with great ease or with great effort, the fact that decryption is absolutely necessary makes it a Practical constraint on the act of gaining access (i.e., effecting the intended audiovisual performance).

the Register as a covered measure under 1201(a), is one example of an Artificial constraint. The effectiveness of a DVD's Region Code depends on a series of operations within a DVD player or DVD-ROM drive, comparing the disc's preferred Region with its own. Those operations are, just like broadcast flag compliance, not absolutely necessary to the act of producing the intended audiovisual performance.¹⁵ The fact that a person may build or buy a device which neglects to perform that comparison suggests only that the prohibition on circumvention may harm users only negligibly; it cannot prove that the measure is not a 1201(a) access-control measure.¹⁶ Likewise, the effectiveness of the broadcast flag (obviously, an Artificial constraint) depends on flag-compliant DTV devices. The simplicity of flag removal and the (presumed) availability of flag-noncompliant DTV devices speak to the minimal harm that 1201(a)'s prohibition inflicts, but do not render the measure outside the bounds of 1201(a).

B. "Requires" may be dictated by external conditions.

Since 1201(a) may properly cover a measure dependent on an Artificial constraint, the next logical objection to 1201(a) protection for flagged DTV questions who imposes that constraint. It is not the "measure" itself which requires flag compliance, but rather a third party – the FCC, or Congress, or an unspoken convention among DTV device manufacturers – operating independently of the copyright owner. The point is that, aside from a constraint imposed by an entity not the copyright owner, there is no requirement that the broadcast flag be identified and adhered to, in the course of performing a DTV transmission. The flag merely indicates a broadcaster's preference, and manufacturers of flag-compliant devices merely accommodate that preference.

¹⁵ On this point, it is easiest to consider a Region-Coded, unencrypted DVD. Such a disc is merely a store of audiovisual data, along with a "flag" indicating a preferred Region.

¹⁶ As a technical note, the Register's 2003 Recommendation endorses acts of "bypassing" Region Coding by using extraregional devices to perform the Region Code comparison, but not by avoiding the comparison altogether. If Region Coding is truly a 1201(a) access control measure, then one should expect that the means or technical sophistication of avoidance is irrelevant to whether 1201(a) is violated. I do not suggest that the Register intentionally promoted illegal conduct; I merely note that my example of "avoidance" is not the same as the one contemplated by the Register.

This argument is not inherently distasteful. But it also pushes DVD Region Coding outside the bounds of 1201(a), since that measure also depends on an external, architectural constraint (DVD devices that recognize and adhere to a disc's Region Code). The copyright owner may indicate its preferred Region, and it may even do so with an explicit knowledge that its indicated preference will almost certainly be respected; but in the end, it is entirely up to DVD device manufacturers whether and how to accommodate that preference. Also foreclosed for 1201(a) protection would be Compact Discs intended to defy playback on a computer – such measures typically depend on an external, architectural constraint (such as the “normal” behavior of a CD-ROM drive, or of an operating system) which the copyright owner does not, and indeed cannot, control, and which is not even remotely static or predictable. And in a curious twist, DVD encryption might lose 1201(a) protection by this reasoning, since its CSS encryption system depends, for its very survival, on an external constraint imposed politely by the grace of the manufacturing industry: blank DVDs and DVD-writing equipment are incapable of writing or storing a CSS disc keyset.¹⁷

Whether a constraint is imposed with, or independent of, the copyright owner's acquiescence does not seem to affect 1201(a) protection.

C. “Requires” may be universally permissive.

One notable distinction between a typical access-control and the broadcast flag is that, while the former may result in denial of access, the process of flag compliance can never produce that outcome. Therefore, it may be concluded, the broadcast flag system “requires” nothing, having no condition upon “gain[ing] access.” A brief examination of typical “denials” betrays the inadequacy of this conclusion. DVD encryption may result in denial of access, but only for an unauthorized DVD copy. Region Coding may result in denial, but only for an imported or exported DVD. Software requiring a dongle may result in denial, but only for an unlicensed installation.

¹⁷ However, there do exist fully-functional blank DVDs and DVD-writing devices upon which this constraint is not imposed. Computer science professor Ed Felton affectionately refers to the vacuum surrounding such consumer-oriented constraints as “the professional devices hole.”

The obvious pattern of “denial” in these cases is a consequence of an activity violative of the copyright holder’s exclusive rights. If infringement is ignored, the result looks very different: a DVD player will never refuse a legitimate DVD; a DVD player will never reject a domestic Region Code; and a licensed software configuration will never fail a dongle check. An intellectually honest comparison of the broadcast flag to those “denials” would examine the flag’s impact on infringing DTV programming – that is, an unauthorized copy or retransmission. So examined, the flag’s purpose to “deny” aligns with the other measures: DTV copied with a flag value of “allow one copy” denies access to subsequent copies; and DTV with a flag value of “allow no copies” denies access to any copy.

Of course, were “effectively controls access” construed by an identifying “authority” phrase, making transactional independence a mandatory condition, then this entire discussion would be irrelevant: DVD encryption, Region Coding, computer-resistant CD Audio, and dongles, without transactionally-independent authority to access, would not be 1201(a) measures. Concession of that point is not seriously anticipated. In short, any plausible argument that the broadcast flag does not “require” flag compliance necessarily disrupts conventional wisdom regarding 1201(a) applications in general and so may not, consistent with prevailing views, be considered. Therefore, the broadcast flag system “requires” recognition, preservation, and adherence.

5. Broadcast Flag Compliance is an “Authorized Process.”

At a very basic level, it is almost beyond question that flag compliance is a process undertaken with the copyright holder’s authority. Any broadcaster who flags a DTV transmission must do so with an explicit, informed knowledge of the procedures which that flag will set in motion, and so must “authorize” those procedures to occur. But, as with the discussion of “requires,” this basic answer trivializes and masks the complexity of the issue.

The real question of whether flag compliance (recognition, preservation, adherence) is a process undertaken “with the authority of the copyright owner” may be expressed more generally for Interactive measures in this way: in the course of interacting with a work to produce an intended user experience (audiovisual performance; program execution; etc.), which processes are undertaken “with the authority of the copyright owner,” and which are not? This profound

question of law, ultimately, is the one which determines whether the broadcast flag system is, or is not, a 1201(a) access-control measure.¹⁸

In exploring this question, note that a “process with the authority of the copyright owner” must have an alternative either in the negative (authorized, vs. not authorized) or in the null (authorized, vs. not requiring authority). Interpreted with a negative-alternate, the statute defines a 1201(a) measure to require a process which the copyright owner has authorized, regardless of whether that authority is “required.” But an authorization not “required” is, in reality, of no consequence at all. The statute would encompass absolutely every process, since a copyright owner’s act of distributing a work, by implication, “authorizes” the receiver to partake in the many complex operations necessary to produce the intended user experience. So broad a reach for 1201(a) cannot have been the intent of Congress.

But to interpret “authorized process” in the null-alternate view yields a more approachable result, since the statute’s reach is confined to a certain type of measure: that is, measures requiring a process, if to perform that process is not merely authorized by the copyright owner but actually requires the copyright owner’s authority. The question then becomes, which processes are those? As a basic copyright matter, a process “requires authority” if it implicates one of the copyright owner’s exclusive rights. But then, none of the measures discussed herein reach into that territory.¹⁹ Fortunately, one may resolve the question in an equitable sense. The purpose of 1201(a) is to remedy a marketplace defect which digital technology amplifies: the inequitable transfer of value resulting from unauthorized (to mean, in general, uncompensated) access. That defect is cured when the value transfer between a user and the copyright owner is equalized: it results in alignment between the value a user gains from experiencing a work, and the value a copyright owner extracts for that experience. A standard for distinguishing an “authorized process,” in the null-alternate view of that term, may therefore be stated in this way: when a measure incorporates a process which, if avoided or bypassed, results in an inequitable transfer of value, then the measure “requires” the copyright holder’s authority. Avoidance of that

¹⁸ The identifying interpretation of “authority” avoids this extremely subjective question by requiring a technological measure to depend on an expression of “authority to access,” a condition which may be revealed through a basic factual inquiry.

¹⁹ Unless, of course, one believes that the act of performing an audiovisual work, or of executing a computer program, can intrinsically violate an exclusive right of the copyright owner. I will leave that particular can of worms undisturbed.

measure yields inequality, and so it is punished. Conversely, if avoiding or bypassing the process does not generate inequality, then the measure does not “require” such authority. To 1201(a), avoidance is irrelevant.

Echoing the previous discussion on transactional independence, a pair of meanings has surfaced for a 1201(a) “authorized process.” Such a process is one which permits an otherwise-infringing act or produces an equitable transfer of value; or, it is absolutely any process at all which the copyright holder anticipates without objection. For the same reasons that not-transactionally independent works are categorically inconsistent with an identifying “authority” phrase, they are categorically inconsistent with a null-alternate “authorized process.” This is proven because, of the measures protecting not-transactionally independent works discussed herein (DVD encryption, Region Coding, dongles, copy-resistant CD Audio), not one, in its ordinary operation, implicates a copyright owner’s exclusive right or produces in an equitable value transfer which did not already exist. So, they are not consistent with the null-alternate view. Those measures do fit quite nicely, however, into the category of “absolutely any process at all,” which flows from the negative-alternate view. Consistent with 1201(a) protection for those measures, and because the flag compliance process is one which the copyright owner both anticipates and finds unobjectionable, a broadcast flag system is an “authorized process” under 1201(a).

This is not to say that the negative-alternate view of an “authorized process,” which produces that result, is necessarily very smart. The discussion in *Reimerdes* on this point captures the fragility of reason surrounding the negative-alternate construction. The court stated that decryption “requires authority,” but it deduced the fact of that “requirement” in an impossibly tenuous way: from the fact of a common licensor (DVD-CCA) shared by a copyright owner (for encryption) and a conventional DVD player manufacturer (for decryption). To deduce that such a link proves whether a process “requires” authority is not a conclusion at all, but rather a self-proving assertion.²⁰ Consider, first: whether a conveyance of decryption authority to third-party licensees was an explicit article of a copyright owner’s DVD-CCA license, the court did not ask. And second: on whether such a link may properly spill into other technologies dependent on common licensure – such as licenses for MPEG-2 video compression and extraction, or for AC-3

²⁰ A more clear example of circular logic cannot be fathomed: Decryption requires authority, because one cannot decrypt except with a license; and one cannot decrypt without a license, because to decrypt requires authority.

“Dolby Digital” audio compression and extraction, or for optical disc manufacture and reading – and thus capture those operations into the reach of 1201(a), the court did not speculate.

In fact, decryption was considered an “authorized process” only because the plaintiffs anticipated, without objection, that co-licensees of CSS technology (conventional DVD player manufacturers) would perform the decryptive operation. The only possible, general rule which may be inferred from the court’s reasoning is exactly the one mandated by the negative-alternate interpretation: a “process with authority” is any process which the copyright holder anticipates and finds unobjectionable.

Comparable reasoning must inform any determination that a Region Code comparison, or a dongle validation, or a CD Audio interaction, is an “authorized process.” They implicate no exclusive right of, and their avoidance inflicts no inequity of value upon, the copyright owner; but each one is a process which the copyright owner anticipates without objection. For the same reasons, and because broadcast flag compliance is exactly identical in these respects, that measure must qualify for protection under 1201(a).