

MOTION PICTURES, MARKETS, AND COPYLOCKS

*Justin Hughes**

INTRODUCTION

There is much to recommend the theme of this conference:¹ conceptualizing law as a “platform” for human activity and, in particular, intellectual property law as a platform for creativity and innovation. For the film industry, it seems obvious that the exclusive rights of copyright law provide the principal *legal* foundation for private investment in *most* audiovisual production—and all the creativity and innovation made possible by that investment. Against the challenge of saying something interesting about what seems like the obvious, this Article has two parts.

Part I ponders how the copyright platform shapes the film industry in the United States and OECD countries through the prism of Nigeria’s audiovisual sector—Nollywood—a film industry that has arisen in an environment without meaningful copyright enforcement. Nollywood is now moving toward distribution channels that better offer the promise of exclusive rights—and the investment and economic possibilities that come with those exclusive rights. But it is Nollywood’s earliest incarnations—as “entertainment in a Hobbesian state”—that show us what cinema culture would look like without the copyright “platform.”

Part II of this Article looks at how one relatively new area of copyright law provides a quietly important “platform” for the current and future success of the world’s audiovisual industries: the legal protection of “technological protection measures” (“TPMs”) or “digital rights management” (“DRM”), i.e., laws that protect the “digital locks” that content owners increasingly use in their distribution business models. The protection of DRM for digital distribution circles back to the future development of Nollywood:

* Hon. William Matthew Byrne Professor of Law, Loyola Law School, Loyola Marymount University. The author thanks Brian H. O’Beirne for research assistance as well as Jesse Fox and Philine Schroeter for their help on an early version of this essay. Thanks also to Fred von Lohman and Mitch Singer for discussions on different technologies related to streaming platforms. The remaining errors are the exclusive intellectual property of the author. Copyright © 2015 by the author. Permission is hereby granted for noncommercial reproduction of this Article in whole or in part for educational or research purposes, including the making of multiple copies for classroom use, subject only to the condition that the name of the author, a complete citation, and this copyright notice and grant of permission be included in the copies.

¹ Content from this Fall 2015 Conference—produced by the Center for the Protection of Intellectual Property (CPIP) at the George Mason University School of Law—is available at *The IP Platform: Supporting Invention & Inspiration*, CTR. PROTECTION INTELL. PROP., <http://cpip.gmu.edu/conferences/2015-fall-conference/> (last visited May 7, 2016).

its prospects for economic growth through better regional and global distribution depend partly on the protection of those same “digital locks.”

I. CULTURAL PRODUCTION WITHOUT EXCLUSIVE RIGHTS—POETRY, ACADEMICS, AND NIGERIAN FILMS

Discussions about the “incentive” structure of copyright law are ubiquitous in legal scholarship,² but we must be careful with how we word (and understand) this idea. There is no problem if we understand the “incentive structure” of copyright to mean that “[c]reative work is to be encouraged and rewarded” by copyright³ and that we are describing a legal platform that “induces creative persons to develop and exercise their talents and thereby avoids the underproduction of . . . original forms of expression.”⁴

But when the “economic incentive view of copyright” is framed as being: “the recognized purpose of the copyright laws” is to “provid[e] creators with a financial incentive to create for the ultimate benefit of the public,”⁵ it starts to sound like copyright *causes* or *triggers* the creativity. Further down this road, we get to the ridiculous comment attributed to Samuel Johnson that “[n]o man but a blockhead ever wrote except for money.”⁶

² For just the tiniest tip of the iceberg of scholarly recognition of the incentive structure of copyright, see Shyamkrishna Balganesh, *Foreseeability and Copyright Incentives*, 122 HARV. L. REV. 1569, 1577 (2009) (“Copyright, it is argued, exists to provide creators with an incentive to create and disseminate their works publicly.”); Stephen Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs*, 84 HARV. L. REV. 281 (1970) (examining the moral and economic rationale for copyright in books); Justin Hughes, *Fair Use Across Time*, 50 UCLA L. REV. 775, 793 (2003) (“If one were to look for an overriding intent vis-à-vis copyright, it is surely that it creates incentives to produce and distribute public goods that otherwise would be underproduced.”); Joseph P. Liu, *Copyright and Time: A Proposal*, 101 MICH. L. REV. 409, 428 (2002) (“The primary policy justification for copyright protection in the United States is the incentive justification.”); Stewart E. Sterk, *Rhetoric and Reality in Copyright Law*, 94 MICH. L. REV. 1197, 1203 (1996) (“[I]t is incentive language that pervades the Supreme Court’s copyright jurisprudence.”); Avishalom Tor & Dotan Oliar, *Incentives to Create Under a “Lifetime-plus-years” Copyright Duration: Lessons from a Behavioral Economic Analysis for Eldred v. Ashcroft*, 36 LOY. L.A. L. REV. 437, 439 (2002) (characterizing “[t]he provision of incentives to create” as “that fundamental goal of copyright law”). See also William Fisher, *Theories of Intellectual Property*, in NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 168 (Stephen R. Munzer ed., 2001) (discussing the theories of intellectual property); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326 (1989) (“Striking the correct balance between access and incentives is the central problem in copyright law.”). But practically everyone who has written about copyright could be added to this list.

³ *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

⁴ William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1659, 1700 (1988).

⁵ *Dawson v. Hinshaw Music Inc.*, 905 F.2d 731, 733-34 (4th Cir. 1990).

⁶ *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994) (quoting 3 JAMES BOSWELL, *THE LIFE OF SAMUEL JOHNSON*, LL.D. 19 (George Birkbeck Hill ed., Clarendon Press 1934) (1791)) (internal quotation marks omitted).

That remark is ridiculous because it is so *obviously* untrue. Lots of the world's great literary and artistic creativity needed and need no financial incentive at all. If literary and artistic production was caused only or principally by *financial incentives*, far fewer people would be in, or even *try* to enter, creative industries. In a developed economy with varied professional opportunities, people work in creative industries primarily for other reasons—the creative process, self-expression, desires for attention and fame, etc. These are the “incentives” that pull someone to filmmaking instead of investment banking, writing music instead of selling real estate, or learning to write software instead of learning to install drywall.

When we talk about the “incentive structure” of copyright [or patent] we are talking about a legal platform that allows someone to create the things that she is otherwise inspired to create—instead of her being forced to do other things to pay the bills. And that means that even without copyright, when people are inspired to be creative we should expect some—indeed a considerable amount of—creative production.

This is clearly the case in areas of original expression where the exclusive rights provided by copyright just cannot provide the “platform” for financial security to pursue some particular creative endeavor. For example, copyright has never provided a strong financial foundation for poetry simply because exclusive rights over poems are not lucrative unless people want poetry enough to support poets. Some of our most important poets supported themselves with completely different professions—Wallace Stevens was an insurance executive and William Carlos Williams was a pediatrician.⁷ Others, like Sylvia Plath, Derek Walcott, and Archibald Macleish, supported themselves with a combination of teaching, fellowship appointments, and office work.⁸ The proceeds from copyright protection would never put enough bread on the table.

Poetry, of course, is pretty “low tech” and has—beyond the poetry sold to high school and university students—a very small base of committed consumers. When we discuss copyright “industries,” our focus is elsewhere: on the production of original expression in the form of prose books, newspapers, audiovisual products, music, and software. Is copyright really the friendly “platform” we assume it is for these industries?

⁷ ELEANOR COOK, *A READER'S GUIDE TO WALLACE STEVENS* 2 (2007) (“In 1916 [Stevens] joined the Hartford Accident and Indemnity Company, where he became a vice-president in the home office in 1934.”); JAMES LAUGHLIN, *REMEMBERING WILLIAM CARLOS WILLIAMS* 11 (1995) (“[Williams was a] [f]ull-time pediatrician as well as an obstetrician.”).

⁸ EDWARD BAUGH, *DEREK WALCOTT*, at ix-x (2006) (describing different positions held by the poet, including as assistant master at St. Mary's College between 1947-50 and 1954-57); JO GILL, *THE CAMBRIDGE INTRODUCTION TO SYLVIA PLATH* 16 (2008) (discussing Plath's career as an instructor at Smith College); GROVER SMITH, *ARCHIBALD MACLEISH* 6 (1971) (noting that after receiving his law degree, MacLeish taught government and practiced law).

A. *One Film Industry Without Copyrights*

Much scholarly discourse in intellectual property depends, implicitly or expressly, on untestable, unknowable counterfactuals (as does Part II of this Article). Sometimes these counterfactuals are straightforward, e.g., *imagine all the cultural materials that would be in the public domain if the copyright term were only life+50?* Sometimes, they are extremely speculative, e.g., *how would creativity look if there were no derivative work right?* How would the software industry look if computer programs had been given a *sui generis* form of protection or only patent protection?

The untestable nature of counterfactuals occasionally leads to extremes. For example, in 2010 a German historian argued that weak copyright was the reason for far more rapid nineteenth-century industrial expansion in Germany than in Britain.⁹ The value a person assigns to such counterfactuals depends on whether her heart and head are more in parlor games or more in policymaking. Instead, consider a counterfactual backed by a significant, “naturally occurring” experiment. The counterfactual is *how would an audiovisual industry form without meaningful copyright protection?* And the real-world experiment is the *enormous* film industry of Nigeria.

The Nigerian audiovisual industry—“Nollywood”—is quite different from the film industries one is accustomed to in OECD countries. Estimates of how many Nollywood films are produced vary significantly—from 800 to 1,500 to 2,500 annually.¹⁰ By some estimates, Nollywood employs over a million people, making it Nigeria’s second or third largest sectoral employer after agriculture (and perhaps after the public sector).¹¹ Total annual revenues for the Nigerian audiovisual industry were estimated at \$590 million U.S. in 2013.¹²

⁹ Frank Thadeusz, *No Copyright Law: The Real Reason for Germany’s Industrial Expansion?*, SPIEGEL ONLINE INT’L (Aug. 18, 2010), <http://www.spiegel.de/international/zeitgeist/no-copyright-law-the-real-reason-for-germany-s-industrial-expansion-a-710976.html> (quoting economic historian Eckhard Höffner as positing that Germany’s economic rise was due to the “incomparable mass of reading material [that] was being produced in Germany,” which, in turn, was due to weak copyright laws).

¹⁰ Mark F. Schultz, *The Nigerian Film Industry and Lessons Regarding Cultural Diversity from the Home-market Effects Model of International Trade in Films*, in TRANSNATIONAL CULTURE IN THE INTERNET AGE 231, 231 (Sean A. Pager & Adam Candeub eds., 2012) (“[Nollywood produces] an output of between 800 and 1500 films a year”); Rebecca Moudio, *Nigeria’s Film Industry: A Potential Goldmine?*, AFRICA RENEWAL ONLINE (May 2013), <http://www.un.org/africa/renewal/magazine/may-2013/nigeria%E2%80%99s-film-industry-potential-gold-mine> (“The Nigerian film industry . . . produces about 50 movies per week”); Sandra Oyewole, *A Peek Inside Nigeria’s Film Industry*, WIPO MAG. (April 2004), http://www.wipo.int/wipo_magazine/en/2014/02/article_0001.html (“[Nollywood] produces on average 1500 films per year.”).

¹¹ Moudio, *supra* note 10 (“Over a million people are currently employed in the industry, making it the country’s largest employer after agriculture.”).

¹² *Id.*

Of course, on paper the 190 million people of Nigeria live under a modern regime of copyright law. Nigeria is a member of the Berne Convention and the Trade-Related Aspects of Intellectual Property or “TRIPS” Agreement,¹³ and Nigeria’s domestic copyright law appears—on the books—compliant with those international standards.¹⁴ But in truth, everyone agrees that there has been little or no copyright enforcement in the “straight to video” market in which Nollywood emerged in the 1990s.¹⁵ One could say that the Nigerian audiovisual market was (and is) beset by *piracy*, but it is easier to say that Nollywood began and flourished in a market where *there was in effect no copyright*.

But how does a creative industry begin and flourish without legally guaranteed exclusive rights? What does “entertainment in a Hobbesian state” look like? For people who work in or write about intellectual property policy, the Nigerian audiovisual industry is a wonderful real world experiment for many important propositions.

One of those propositions is that technologically enabled declining costs of content production enable new market entrants and diminish many of the gatekeeper function of entities with expensive facilities. This same phenomenon is occurring in the music sector in North America and Europe as more and more artists succeed with what are essentially “home recordings.” As David Byrne noted in 2013, “Home-studio recordings can now sound as good as the big-name studios, and the lower pressure (and less expensive) vibe in a home environment is often more conducive to creativity.”¹⁶

¹³ Nigeria became a party to the Berne Convention for the Protection of Literary and Artistic Works on 14 September 1993. *Berne Convention for the Protection of Literary and Artistic Works*, WORLD INTEL. PROP. ORG., <http://www.wipo.int/export/sites/www/treaties/en/documents/pdf/berne.pdf> (last visited May 7, 2016) (listing all contracting parties to the Berne Convention as of January 15, 2016). Nigeria is also a signatory of the Trade-Related Aspects of Intellectual Property (TRIPS) Agreement. See *Understanding the WTO: The Organization: Members and Observers*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited May 8, 2016).

¹⁴ Kunle Ola, *Evolution and Future Trends of Copyright in Nigeria*, in COPYRIGHT PERSPECTIVES: PAST, PRESENT AND PROSPECT 97, 119 (Brian Fitzgerald & John Gilchrist eds., 2015) (“Nigeria as a developing country has complied with most of the[] requirements [of the Agreements on Trade Related Aspects of Intellectual Property]”). See generally JOHN O. ASEIN, NIGERIAN COPYRIGHT: LAW & PRACTICE (2d ed. 2012).

¹⁵ Oyewole, *supra* note 10 (“The industry’s phenomenal growth was triggered in 1992 with the film *Living in Bondage*, the first commercially successful [Nigerian] movie shot straight-to-video. Direct-to-video . . . distribution is a hallmark of the Nigerian industry.”).

¹⁶ DAVID BYRNE, HOW MUSIC WORKS 174 (2012). Byrne describes how his early albums were done in commercial studios, but his vocals for the 2002 hit “Lazy” were done on a laptop “and no one ever complained that the vocal sounded like it had been recorded on a laptop. The homemade recording had quietly passed the litmus test.” *Id.* at 180. He recounts “home studios” of Morcheeba, Devo, and Black Cat Orchestra. *Id.* at 175. For a new artist who achieved commercial success recording herself with GarageBand software, see Mark Yarm, *Despite Electro-Pop Stardom, Grimes Keeps It Fiercely*

In the case of the Nigerian audiovisual industry, observers agree that relatively inexpensive video cameras and easy transfer to VHS videocassettes (and later DVDs) eliminated the technological and capital barriers of a celluloid-based audiovisual industry, creating a sector of cultural production open to virtually anyone.¹⁷ As John McCall, a longtime Nollywood observer has noted, “Virtually anyone who can rent the equipment for a few days can become a Nollywood producer.”¹⁸

More importantly, the Nollywood experiment confirms what students of intellectual property have long believed: that some “natural” exclusivity is temporarily available in “first mover” advantages.¹⁹ Observers agree that without any meaningful copyright enforcement, the Nigerian audiovisual industry developed almost purely on first-mover advantages: a film producer has a window of *two weeks* or less²⁰ in which to recoup his investment and make any profit before piracy overwhelms legitimate sales that would carry any premium:

As soon as a film is released, copyright thieves rip it off. It takes the pirates just two weeks to copy a new film and distribute it across Africa. The merchants must take their

Grimy, WIRED (Oct. 23, 2015), <http://www.wired.com/2015/10/grimes-art-angels/> (describing success and recording practices of electro-pop musician “Grimes,” a.k.a. Claire Boucher).

¹⁷ See Schultz, *supra* note 10, at 243 (“[T]he introduction of relatively inexpensive video cameras and production was what lowered barriers sufficiently to allow the Nigerian film industry to get started.”); Jonathan Haynes, *Nollywood in Lagos, Lagos in Nollywood Films*, 54 AFRICA TODAY 131, 134 (2007) (“Cheap and easily operated video technology allowed [film] to arise as an informal-sector activity”); Moudio, *supra* note 10 (stating that Nollywood films “gained popularity during the digital revolution of the early 1990s when camcorders replaced 35-millimeter film cameras, and digital systems replaced celluloid as recording devices. At the time, . . . Nigeria continued to use inexpensive VHS tapes and players that were easily accessible and affordable to consumers.”); see also Tunde Kellami, *Spielberg & I: The Digital Revolution*, in NOLLYWOOD: THE VIDEO PHENOMENON IN NIGERIA 90 (Pierre Barrot ed., 2008).

¹⁸ John C. McCall, *The Pan-Africanism We Have: Nollywood’s Invention of Africa*, 28 FILM INT’L 92, 96 (2007).

¹⁹ See, e.g., WILLIAM M. LANDES & RICHARD A. POSNER, *THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW* 42 (2003) (“Copying takes time, so there will be an interval during which the original publisher will not face competition. . . . But modern technology has reduced the time it takes to make copies, as well as enabled perfect or near-perfect copies to be made at low cost . . .”).

²⁰ Schultz, *supra* note 10, at 240 (“Piracy severely constrains the size of the market for each film in Nigeria, limiting them to the market allotted by first-mover advantage. A filmmaker has about a two-week window before piracy forecloses further sales, and some likely competition with pirates or dishonest distributors during those first two weeks.”); Moudio, *supra* note 10 (“The films . . . are profitable within two to three weeks of release.”). *But see* Oyewole, *supra* note 10 (“Within hours of a film’s release pirates are selling bootleg copies for a fraction of its retail price.”).

money during that fortnight, known as the “mating season”, before their discs become commodities. As soon as the mating season is over they start thinking about the next film.²¹

During the initial flowering of Nollywood, the first-mover advantages have been enhanced by an otherwise barren entertainment environment—bad state-run television and poor Internet connections²²—creating a fertile environment for a home video rental/sale market.²³

Because being first in the market has been virtually the only basis for exclusivity, the “mating season” window puts a cap on how much can rationally be invested in a Nollywood production. Depending on the source, that ceiling can be as low as \$25,000 U.S. or as “high” as \$100,000 U.S.²⁴ And this cap on investment has also meant a cap on everything else. As *The Economist* described the situation in 2010, “Studios, both in the physical and the corporate sense of the term, are unknown. There are no lots, no sound stages and no trailers for the stars.”²⁵ There are usually no sets²⁶ and little costuming.²⁷ Casting can be last minute,²⁸ and acting salaries are modest.²⁹

In addition to putting a ceiling on investment and, therefore, every aspect of quality, the lack of effective copyright seems to produce a faster cycle of content production and distribution.³⁰ That is, if your only period to recoup investment is during a short window after introducing your product to the market, then continued cash flow depends on the introduction of new content at a fairly rapid clip. As Jonathan Haynes describes it, “The most workable business strategy is to make films as cheaply and quickly as possible, shooting in a week, trying to recoup the investment in the two weeks

²¹ *Lights, Camera, Africa: Movies Are Uniting a Disparate Continent, and Dividing It Too*, ECONOMIST (Dec. 16, 2010), <http://www.economist.com/node/17723124/print> [hereinafter *Lights, Camera, Africa*].

²² *Id.* (“Atrocious state-run television and slow internet connections mean there is little competition for entertainment.”).

²³ Oyewole, *supra* note 10 (“Revenues are almost exclusively derived from home video rentals and sales and this has, to a large extent, worked in their interests.”).

²⁴ Moudio, *supra* note 10 (“On average, producing a movie in Nigeria costs between \$25,000 and \$70,000, says the British Broadcasting Corporation.”); *Lights, Camera, Africa, supra* note 21 (“All scenes are shot on location and with a shoestring budget of no more than \$100,000.”).

²⁵ *Lights, Camera, Africa, supra* note 21.

²⁶ *But see* John C. McCall, *Nollywood Confidential: The Unlikely Rise of Nigerian Video Film*, 95 TRANSITION 98, 102 (2004) [hereinafter McCall, *Nollywood Confidential*] (describing film production where “[s]et builders erected a traditional village”).

²⁷ *See id.* at 101.

²⁸ *See id.* at 100 (describing arriving at a film site where “they were still casting the movie, though shooting was scheduled to begin later that week”).

²⁹ Moudio, *supra* note 10 (“Nollywood actors’ incomes are low. Even the most popular get paid between \$1,000 and \$3,000 per film. Only a few can claim higher earnings.”).

³⁰ Schultz, *supra* note 10, at 233 (“[P]iracy limits and shapes supply, likely yielding far more films but with lower-value creative inputs.”).

or so before the pirates can catch up, and then moving on to another film.”³¹ In other words, if there can be such a thing as cultural “over-production,” that has arguably happened with Nollywood content.

At the same time, in its early incarnation, Nollywood has done exactly what creative industries are supposed to do: capture, echo, elaborate, and disseminate the narratives of the culture from which the creators come.³²

B. *Fade-Out on the Nollywood Experiment?*

In recent years, the Nigerian audiovisual industry has started looking more like its California- and Mumbai-based counterparts. Distribution on more piracy-proof platforms is slowly nudging Nollywood toward a more traditional profile for an audiovisual industry. Those platforms are cinemas, satellite broadcasting, and online digital distribution.³³

In his presentation at the 2015 CPIP conference, Ben Sheffner described copyright protection *globally* as “great on paper” but having real “challenges in practice.”³⁴ In contrast to “real problems online” with enforcement, he noted “excellent enforcement in [the] theatrical market.”³⁵ Accepting all these points, it is important to remember that in the theatrical market, *real property laws*, not copyright, are the principle enforcement of exclusivity: if a consumer does not buy a ticket to the cinema, the consumer is a trespasser. If the motion picture is embedded on film stock or in a digital file on a chattel, the copy is behind locked doors in the projection room. Anti-camcording laws can be an important part of preventing copying,³⁶ but

³¹ Jonathan Haynes, *Video Boom: Nigeria and Ghana*, 3 POSTCOLONIAL TEXT 1, 3 (2007).

³² McCall, *Nollywood Confidential*, *supra* note 26, at 100, 109 (“[Y]oung people in Lagos . . . admitted that most of what they knew about village life was gleaned from watching the videos. . . . [And] [i]n Igboland [videos] have become a key reference point for discussions about what it means to be Igbo in a modern world.”).

³³ See Oyewole, *supra* note 10.

³⁴ Ben Sheffner, Vice President Legal Affairs, Motion Picture Ass’n of Am., Presentation at the 2015 CPIP Conference, George Mason University School of Law: IP and the Movies We Watch (Oct. 1, 2015), available at *The IP Platform: Supporting Invention & Inspiration*, CTR. PROTECTION INTELL. PROP., <http://cpip.gmu.edu/conferences/2015-fall-conference/> (last visited May 7, 2016).

³⁵ *Id.*

³⁶ Such laws exist in a wide variety of jurisdictions. See, e.g., BOC Editorial, *Japan Passes Anti-camcording Law*, BUSINESSOFCINEMA.COM (May 26, 2007), <https://businessofcinema.com/bollywood-news/japan-passes-anticamcording-law/18637>; Patrick Frater, *Malaysia Passes Anti-camcording Law*, FILM BUS. ASIA (Dec. 23 2011), <http://www.filmbiz.asia/news/malaysia-passes-anti-camcording-law>; Etan Vlessing, *Canada Passes Anti-camcording Law*, HOLLYWOOD REP. (June 23, 2007), <http://www.hollywoodreporter.com/news/canada-passes-anti-camcording-law-140238>. In the United States, a majority of states make camcording in a cinema illegal. See, e.g., ARIZ. REV. STAT. ANN. § 13-3723 (2015); CAL. PENAL CODE § 653z (West 2016); FLA. STAT. § 540.12 (2015); MASS. GEN. LAWS ch. 266, § 143F (2005); OHIO REV. CODE ANN. § 2913.07 (West 2016); 18 PA. CONS. STAT. § 4116.1 (2016).

the terms and conditions that the cinema owner imposes on the ticket purchaser for access to the real property of the cinema can achieve a similar result.

Nollywood emerged in its direct-to-video form at a time when cinemas had all but ceased to exist in urban Nigeria,³⁷ but in recent years, Nigeria has experienced a surge of new cinema openings.³⁸ This development can provide Nollywood with a revenue source where exclusivity is better protected. (The new openings have also prompted Nigeria to see a cultural phenomenon closely attached to the cinema: the movie “premiere.”) In the early years of the twenty-first century, Nollywood films also started to have a presence on satellite television,³⁹ another distribution platform that can generate licensing revenues.

Finally, video streaming platforms offer Nollywood a traditional copyright-based revenue stream. In 2011, iROKOTv launched a video streaming platform for Nigerian films⁴⁰ with an eight million dollar investment from an American hedge fund,⁴¹ and in 2015 Netflix began including some Nollywood films in its offerings.⁴² With estimates of Nigerians in diaspora ranging from five to fifteen million⁴³ and the affluent components of this diaspora located in Anglophone countries outside Africa, such video streaming platforms could cultivate a market that has been underserved even by piracy.

Of course, legitimate streaming services, like NetFlix and iROKOTv, that pay Nigerian filmmakers will have to compete online with unauthorized BitTorrent sources and pirate-streaming services that will also provide

³⁷ As of 2010 *The Economist* reported, “With a population of 15m, Lagos has just three working cinemas.” *Lights, Camera, Africa*, *supra* note 21.

³⁸ Oyewole, *supra* note 10 (reporting that the Nigerian government has licensed “up to 80 fee paying cinemas”).

³⁹ *Id.* (describing “[t]he launch of the first Africa Magic Channel on Digital Satellite Television (DStv) in 2003”).

⁴⁰ One can subscribe to the platform at <http://irokotv.com/>. As of December 2015, subscribers were offered different payment options, including \$US 42 for a year subscription and \$US 2.99 for a daily subscription. See *iROKOTv Terms of Use*, IROKOTV.COM, <http://irokotv.com/about/terms> (last visited May 7, 2016).

⁴¹ Oyewole, *supra* note 10.

⁴² George Platman, *From Nigeria to Netflix: African Cinema Goes Global*, TELESURTV.NET (Apr. 21, 2015), <http://www.telesurtv.net/english/analysis/From-Nigeria-to-Netflix-African-Cinema-Goes-Global-20150421-0024.html> (“Finally, 2015 has seen the big transition from Nollywood-specific streaming sites to the multimedia international Netflix.”); see also *Netflix Shows Nigerian Films but . . .*, JOVIBABS (Sept. 26, 2015), <http://www.jovibabs.com/netflix-shows-nigerian-films-but/> (“[T]he American VOD giant Netflix has acquired some Nigerian films to show on their platform . . .”).

⁴³ *The Nigerian Diaspora*, NIGERIANDIASPORA.COM, <http://nigeriandiaspora.com/nigerian-diaspora.php> (last visited Mar. 5, 2016) (“Estimates of the size of the Nigerian Diaspora vary greatly and range from about 5 million to 15 million people.”); Oyewole, *supra* note 10 (“iROKOTv report[s] a global audience of 6 million in 178 countries . . .”).

Internet access to Nollywood content. The Nigerian film industry *wants* meaningful copyright enforcement, and, not surprisingly, Nigeria's political leaders have responded—at least in words.⁴⁴ Enforcement against unauthorized digital distribution is part of an environment in which authorized streaming services will be able to continue in the long-term to pay for Nigeria's audiovisual production.

And this development leads to the *connection* between the two “new” Nollywood revenue sources, cinema and streaming: that connection is technological protection measures (“digital locks”) and the laws that protect the digital locks. The use of “digital locks” by content owners and distributors has made it possible to have delivery systems, like Netflix and iROKOtv, that create a “cinema” experience on the Internet where consumers can pay to enjoy an audiovisual work but pay less than if they were receiving a permanent copy of that audiovisual work.

II. THE PRESENT DAY IMPORTANCE OF § 1201

As the ease of digital reproduction and distribution started to become clear in the 1990s, copyright owners concluded that future content delivery systems were likely to use “technological measures,” “technological protection measures” (“TPMs”), or “digital rights management” (“DRM”) to safeguard content.⁴⁵ These digital locks were already familiar in the form of password-protected sites like Westlaw and LEXIS/NEXIS as well as scrambled satellite transmissions. In 1996, a new multilateral intellectual property agreement—the World Intellectual Property Organization

⁴⁴ *Nigeria's Muhammadu Buhari Vows to 'Save' Nollywood from Piracy*, BBC (July 15, 2015), <http://www.bbc.com/news/world-africa-33536247>.

⁴⁵ The terminology shifted, almost oddly, in only a few years. The dominant legal term has been “technological measures.” See Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.); World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 36 I.L.M. 65 [hereinafter WCT]; Directive 2001/29/EC of the European Parliament and of the Council, of 22 May 2001, on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, art. 6, ¶ 39, 2001 O.J. (L 167) 10, 13. But in public discussions, this phrase quickly morphed into “technological protection measures” and now “digital rights management.” Note also that digital rights management, also known as “DRM,” is arguably broader in that it can include usage information or embedded metadata that does not actually control the activity. See, e.g., Symposium, *The Law and Technology of Digital Rights Management: Foreword*, 18 BERKELEY TECH. L.J. 487, 488 (2003) (“Generally speaking, DRM systems consist of ‘secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works.’ In other words, DRM systems provide a means of expressing usage rules, a means of associating those rule with content, and frequently, a means of enforcing these rules by preventing actions that the usage rules do not explicitly permit.” (footnote omitted) (quoting Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management*, 15 HARV. J.L. & TECH. 41, 48 (2001))).

(“WIPO”) Copyright Treaty (“WCT”)—was completed.⁴⁶ The WCT “updated” international copyright law in many ways including express protection of software, a new right of “making available,” and a general obligation to protect TPM/DRM.⁴⁷

Once the WCT was completed, copyright policymakers in the United States debated how to draft implementing legislation as part of U.S. ratification of the new treaty. The resulting legislation—with the addition of new “safe harbors” for internet service providers—was the 1998 Digital Millennium Copyright Act⁴⁸ (“DMCA”). After the DMCA’s passage, there was a flurry of critical commentary, particularly focused on the provision concerning digital locks: § 1201. Section 1201 outlaws “circumvention devices”—digital lock picks—used against any DRM that protects copyrighted works, whether the DRM protects a traditional copyright right or controls “access” to a work.⁴⁹ Section 1201 also forbids the *act* of digital lock picking when the DRM secures *access* to a copyrighted work.⁵⁰ The following table shows the matrix produced by § 1201:

	DRM controls access	DRM controls 106 right
Act of breaking DRM	Forbidden by § 1201(a)(1)	[Permitted]
Making/distributing device to break DRM	Forbidden by § 1201(a)(2)	Forbidden by § 1201(b)

Thus, § 1201(a)(1) creates a sort of “circumvention liability for ‘digital trespass’”⁵¹—that is, gaining access to digital content that one was not au-

⁴⁶ See generally WCT, *supra* note 45.

⁴⁷ Article 11 of the WCT provides that “[c]ontracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.” WCT, *supra* note 45, art. 11.

⁴⁸ Pub. L. No. 105-304, 112 Stat. 2860 (1998).

⁴⁹ 17 U.S.C. § 1201(a)(2), (b)(1) (2012). Sections 1201(a)(2) and 1201(b)(1) have parallel structures, each providing that “[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof” that is primarily designed or produced to circumvent digital locks, has “has only limited commercially significant purpose or use other than to circumvent” digital locks, or is knowingly marketed “for use in circumventing” a digital lock. *Id.* Section 1201(a)(2) sets out these prohibitions in relation to “access” controls and § 1201(b) in relation to digital locks that control reproduction or other activities that are exclusive rights of the copyright holder. *Id.*

⁵⁰ *Id.* § 1201(a)(1)(A) (“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”).

⁵¹ Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1196 (Fed. Cir. 2004).

thorized to access, while § 1201(a)(2) and § 1201(b) create “trafficking liability”⁵² for digital-lock picks and digital-lock picking services that would facilitate copyright infringement by others.⁵³

While Congress clearly intended to “back[] with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections,”⁵⁴ § 1201 sets out a complex and nuanced menu of what is prohibited and what is permitted in relation to digital locks protecting copyrighted works. For example, once a consumer has legitimate “access” to a work, the § 1201 provisions do *not* forbid the picking of a “digital lock” that controls further copying of a work, i.e., a lock that controls the exercise of the § 106 right of reproduction.⁵⁵ This structure attempts to draw a rough parallel to traditional means of content delivery: (a) once the consumer has legitimate access to a work, many activities that might be prima facie violations of § 106 rights may also be *fair uses*, but (b) there remains no fair use right of access—one can plead fair use neither for sneaking into a cinema nor for ripping the plastic wrapping off a not-yet-purchased magazine or CD.⁵⁶ The § 1201 provisions also include a set of complex exceptions and a regulatory mechanism for further exceptions—all of which have been the subject of extensive commentary.⁵⁷

Of course, the two types of DRM overlap to some degree, and a vast menagerie of different technologies to protect content—far beyond firewalls and scrambled satellite signals—emerged after 1998.⁵⁸ If the technology is intended to regulate access to a copyrighted work *and/or* to regulate the reproduction, distribution, or public performance of that work, it arguably falls under § 1201 as DRM.⁵⁹

⁵² *Id.*

⁵³ In the apt description of one court:

[T]he Act first prohibits the *act* of circumventing any programs or measures intended to control access to a protected work; second, it makes it unlawful to manufacture or sell technologies designed to circumvent such measures; and third, it prohibits manufacturing, selling or providing devices or technologies that are designed to circumvent protections intended to safeguard a copyright owner’s rights.

Ford Motor Co. v. Autel US Inc., No. 14-13760, 2015 WL 5729067, at *5 (E.D. Mich. Sept. 30, 2015).

⁵⁴ Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 458 (2007) (quoting Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001)) (internal quotation marks omitted).

⁵⁵ *Chamberlain Grp. Inc.*, 381 F.3d at 1193.

⁵⁶ *Id.* at 1185.

⁵⁷ See, e.g., Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121, 144 (2006).

⁵⁸ One review article notes that TPMs “range from the basic to the sophisticated” and include “password protection, copy protection, encryption, digital ‘watermarking’ and, increasingly, rights management systems incorporating one or more of the foregoing.” June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 391-92 (2004).

⁵⁹ *Id.* at 389.

On the whole, scholarly discourse about § 1201 has been negative.⁶⁰ Straightforward textual analysis of the § 1201 provisions did reveal legitimate concerns based on reasonably foreseeable fact patterns.⁶¹ But other commentary was more strident. According to some of this discourse, the DMCA anti-circumvention provisions were going to “chill” innovation and competition so badly⁶² that it is really unclear how now—eighteen years later—we actually have smartphones, tablets, wifi, Facebook, the blogosphere, Google, drones, Instagram, ubiquitous GPS, fledgling driverless cars, and synthetic biology.

In fairness, bad guesses can be found on all sides. In their 2003 book on the economics of intellectual property, William Landes and Richard Posner wrote the following after discussing other commentators’ assumptions about DRM:

This, however, assumes that the technology is adopted when the copyrighted work is first created. It is more likely to be adopted shortly before the copyright expires. Until then the copyright owner may be quite content with enforcing his legal remedies.⁶³

This scholarly “more likely” scenario was already wildly at odds with reality: by 2003, tens of millions of DVDs with “Content Scramble System” encryption had been sold,⁶⁴ not to mention tens of millions of copies of vid-

⁶⁰ Or, more genteelly, “[T]he DMCA has been especially controversial in academic settings.” Karl Manheim, *Introduction: At the Crossroads of Law and Technology*, 25 *LOY. L.A. ENT. L. REV.* 1, 4 (2004).

⁶¹ For example, textual analysis made it obvious that the § 1201(a) prohibition on circumventing access controls could give the copyright owner a cause of action where she would have otherwise had none vis-à-vis § 106 or any other provision of the Copyright Act. See e.g., R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Laws?*, 18 *BERKELEY TECH. L.J.* 619, 626 (2003).

⁶² See Zoe Lofgren, *Edited Transcript of the David Nelson Memorial Keynote Address: A Voice from Congress on DRM*, 18 *BERKELEY TECH. L.J.* 495, 496 (2003) (“[T]he DCMA has . . . had a number of adverse affects [sic] on consumers and entrepreneurs.”); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 *BERKELEY TECH. L.J.* 519, 546 (1999) (anticipating a “chilling effect on legitimate activities”); *id.* at 557 (“[Anti-circumvention provisions] are likely to have harmful effects on competition and innovation in the high technology sector.”); Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 *SCIENCE* 2028 (2001), <http://science.sciencemag.org/content/sci/293/5537/2028.full.pdf>; Peter K. Yu, *Digital Copyright and Confuzzling Rhetoric*, 13 *VAND. J. ENT. & TECH. L.* 881, 929 (2011) (“[A]nti-circumvention laws . . . have brought about many unintended consequences, chilling innovation and competition . . .”); Derek J. Schaffner, Note, *The Digital Millennium Copyright Act: Overextension of Copyright Protection and the Unintended Chilling Effects on Fair Use, Free Speech, and Innovation*, 14 *CORNELL J.L. & PUB. POL’Y* 145, 147 (2004) (“[DCMA] grants too much power to the copyright holder and thus creates a chilling effect on fair use, free speech, future innovation, and competition.”).

⁶³ LANDES & POSNER, *supra* note 19, at 45.

⁶⁴ Greg Tarr, *DVD Group Challenges NPD Sales Report for 2000*, *TWICE* (Feb. 12, 2001), <http://www.twice.com/news/audiovideo/dvd-group-challenges-npd-sales-report-2000/39698> (finding that 2000 sales figures of DVDs reached at least 6,625,617).

eogames and software—almost all for works nowhere near “shortly before the copyright expires.”⁶⁵

Now approaching two decades since the DMCA’s passage, we do not have much empirical knowledge on how its provisions have affected the digital, networked environment. In the case of the § 512 notice-and-takedown provisions, we know *some things* about the amount of takedown notices coursing through the system. For example, we have the laudable statistical reporting on § 512(d) “information location tool” takedown notices from Google’s Transparency Report.⁶⁶ There have also been some bona fide efforts to analyze the quality of takedown notices (and therefore their impact on free expression)⁶⁷ but with small datasets that seem to be too dwarfed by the actual level of notice-and-takedown activity to be statistically meaningful.⁶⁸

Yet our efforts to study and understand the impact of the § 512 provisions vastly exceeds what we have done to try to understand how § 1201 has affected both the protection of copyright and the digital, networked environment. After its initial spat of scholarly bad publicity, § 1201 seems to be largely forgotten. For example, in a 2006 paper, Gigi Sohn, then executive director of the advocacy group Public Knowledge, described different deals between technology and content companies visible at the 2006 Consumer Electronics Show.⁶⁹ From her survey, Ms. Sohn concluded, “[DRM] tools will protect some of [the] content, and consumers can decide whether that protection is flexible enough for their needs,” and “[t]he market for delivering content digitally over new technologies is working.”⁷⁰ In

⁶⁵ LANDES & POSNER, *supra* note 19, at 45.

⁶⁶ *Copyright Removal Requests*, GOOGLE TRANSPARENCY REPORT, <https://www.google.com/transparencyreport/removals/copyright/?hl=en> (last visited May 8, 2016).

⁶⁷ See, e.g., *About*, THE TAKEDOWN PROJECT, <http://takedownproject.org/about> (last visited Feb. 20, 2016).

⁶⁸ For example, on May 8, 2016, the Google Transparency Report stated that Google has received requests for the § 512(d) “takedown” or disablement of search-result links to 94,064,232 discrete URLs appearing in Google search results. *Copyright Removal Requests*, GOOGLE TRANSPARENCY REPORT, <https://www.google.com/transparencyreport/removals/copyright/?hl=en> (last visited May 8, 2016). Two years earlier, in a one-month period in October-November 2014, Google reported receiving notices requesting § 512(d) takedown of 40,356,438 discrete URLs. *Id.* As of the time of this publication, a considerably larger scale study has been released. See JENNIFER M. URBAN, JOE KARAGANIS & BRIANNA L. SCHOFIELD, NOTICE AND TAKEDOWN IN EVERYDAY PRACTICE (2016), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628. The study was funded by Google and the Sloan Foundation. The author has not yet reviewed the Urban, Karaganis, and Schofield study.

⁶⁹ Gigi B. Sohn, *Don’t Mess with Success: Government Technology Mandates and the Marketplace for Online Content*, 5 J. ON TELECOMM. & HIGH TECH L. 73, 73-74 (2006).

⁷⁰ *Id.* at 74.

the next line of the paper, she writes that “[a]ll of these great developments happened without government intervention.”⁷¹

Of course, there was government intervention—with both the § 512 notice-and-takedown and § 1201 digital-lock provisions. So it is quite interesting to read an influential advocate of consumer interests in information products having such an accepting view of the regulatory environment created by the § 1201 provisions.

The remainder of this Article proposes that despite the wide variety of DRM, § 1201’s interaction with our digital environment has broken into two general zones. The first zone encompasses the very visible controversies and litigations over what one might call “discrete copy” TPM. Indeed, these DRM are how many understand § 1201 today. In this area, many digital-lock systems have failed and many have succeeded. And as is often the case in life, the DRM systems that failed tended to fail spectacularly, while the DRM systems that succeeded usually did so quietly.

In a second realm, § 1201 protects the integrity of streaming platforms used by Netflix, Hulu, HBO Now, Spotify, Amazon Prime, and scores of other commercial streaming services.⁷² Sitting in the background, § 1201 *may* have prevented an ugly technological arms race between browser makers, player platforms, hackers, etc. Section 1201 helps make it possible to have the “cinema” of the Internet remain a discrete form of business and for Apple to have iTunes and Apple Music as separate offerings.

A. “Discrete Copy” TPM

Much of the policy discussion and scholarly commentary of DRM has centered on digital locks that come with discrete copies of works that are transferred to end-users, either through physical media or Internet download. The discrete copy must interact with a player device that the consumer already owns. The player device may be “dedicated” in the sense of a PlayStation or Xbox system or “general”—as when a consumer wants to play a CD on the CD drive of a general-purpose personal computer or an .mp3 download on Windows Media Player or iTunes.

⁷¹ *Id.* Later in the same essay she writes, “Content companies are increasingly adopting copy protection and other digital rights management tools in the marketplace, without any government intervention.” *Id.* at 85.

⁷² Meg James & Yvonne Villareal, *A New Streaming Television Landscape*, L.A. TIMES (Jan. 4, 2016), <http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-new-streaming-television-landscape-html-htmlstory.html> (describing some of the “[m]ore than 100 Internet video streaming services . . . now available”); Meg James & Yvonne Villareal, *Cord Cutters Face a Sea of Streaming Options*, L.A. TIMES (Jan. 1, 2016), <http://www.latimes.com/entertainment/envelope/cotown/la-et-01013-ct-ott-mania-20151229-story.html>.

1. “Dedicated” or “Unitary” Eco-System TPM

A ubiquitous form of discrete-copy TPM consists of some code on the discrete copy that the player verifies. This “handshake” verification is the TPM on the Sony PlayStation and other videogame consoles.⁷³ In other words, the player device checks that the loaded, discrete copy is an *authorized* copy of the content.

In the case of video game systems, Sony, Microsoft, and Nintendo have been very successful in defending their respective game platforms against distributors and installers of “modification chips” (“mod chips”) that allow people to play unauthorized games on the PlayStation, Xbox, and Wii game platforms.⁷⁴ Consumers use these mod chips “to fool or bypass a game console’s security measures and enable users to run software for which the console was not originally intended.”⁷⁵ Mod chips represent a good example of how “access” and “§ 106 right” DRM overlap. Viewed as an access control measure, the DRM prevents access to *unauthorized copies*, but the actual effect of this DRM is to suppress the *reproduction and distribution* of these pirate copies because consumers will not purchase pirate copies if they will not play on the game console.⁷⁶

In another type of discrete-copy DRM, the content on the copy is encrypted and the player has a proprietary capacity to decrypt the content: this is the model of DRM on DVDs.⁷⁷ In 1996, Japanese electronics manufacturers and the U.S. motion picture studios agreed on an encryption standard for the new DVD technology called Content Scramble System (“CSS”).⁷⁸ Viewed simply as an encryption technology, CSS looks like an access control measure, but the license to use the CSS decryption keys requires the

⁷³ Aaron K. Perzanowski, *Rethinking Anticircumvention’s Interoperability Policy*, 42 U.C. DAVIS L. REV. 1549, 1572, 1590 (2009).

⁷⁴ *United States v. Reichert*, 747 F.3d 445, 448 (6th Cir. 2014) (successful criminal prosecution of man providing service installing mod chips in Wii and Xbox systems); *Sony Comput. Entm’t Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 959, 968 (N.D. Cal. 2006) (default judgment under § 1201 for trafficking in mod chips); *Sony Comput. Entm’t Am., Inc. v. Filipiak*, 406 F. Supp. 2d 1068, 1070, 1074 (N.D. Cal. 2005) (statutory damages against defendant who agreed to consent judgment that stipulated liability for installation of mod chips).

⁷⁵ *Reichert*, 747 F.3d at 449.

⁷⁶ This point was explored at length in Judge Kevin Lindgren’s opinion in an Australian decision on the mod chips. *Kabushiki Kaisha Sony Comput Entm’t v Stevens*, [2003] 132 FCR 31 (Austl.). The applicable Australian statute at the time protected digital locks that “prevent[ed] or inhibit[ed] the infringement of copyright.” *Id.* ¶ 43. The trial court concluded that the Sony DRM “handshake” did not literally prevent reproduction, but the appellate panel reversed, finding that the effect of the Sony system was to “inhibit” unauthorized reproduction. *Id.* ¶¶ 1-2.

⁷⁷ Besek, *supra* note 58, at 448.

⁷⁸ Details here are drawn from Judge Lewis Kaplan’s careful exposition in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 308 (S.D.N.Y. 2000), *aff’d sub nom.* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

manufacturer of the playing device to ensure that the player does not provide a “digital output that could be used in copying protected DVDs.”⁷⁹ So as deployed in the marketplace, CSS has been both “an access control and copy prevention system for DVDs.”⁸⁰

It cannot be seriously questioned that consumers have generally accepted the digitally locked content on DVDs and videogames. In the world of audiovisual products, U.S. sales of digitally locked DVDs went from 2 million units in 1997 to 1.2 billion in 2007.⁸¹ More importantly, during this period, recorded VCR sales in the United States (an unprotected format) declined 98.1 percent while DVD sales grew 113.9 percent⁸²—a clear pattern of consumption substitution. Although sales of DVDs have declined in recent years—from competition with Blu-ray and digital downloads⁸³—the top 100 film titles still sold over 76.5 million DVD units in the United States in 2015.⁸⁴ That is a lot of consumer acceptance of DRM. In the world of videogames, dedicated, closed formats and platforms with technological protection measures seem to have surpassed unprotected or substantially less-protected videogame entertainment.⁸⁵ In both cases, DRM-protected formats may have had significant content or experience improvements (extra materials and scene selection with DVDs). But even making this assumption, there is no evidence of any substantial consumer resistance to DRM that slowed the sales of the digitally locked format.

2. When “Discrete Copy” TPM Failed—Spectacularly

At the other end of the spectrum, the market for discrete, digital copies of sound recordings unquestionably became the poster child for troubled DRM.

⁷⁹ *Id.* at 310 (“[M]anufacturers may not, consistent with their licenses, make equipment that would supply digital output that could be used in copying protected DVDs. Licenses to manufacture compliant devices are granted on a royalty-free basis subject only to an administrative fee. At the time of trial, licenses had been issued to numerous hardware and software manufacturers . . .” (footnotes omitted)).

⁸⁰ *Id.* at 308 (“CSS, or Content Scramble System, is an access control and copy prevention system for DVDs . . .”). That a single DRM system would have both effects was recognized quite early. *See* Reese, *supra* note 61, at 650-51, 651 n.107.

⁸¹ Over 7 billion such DVDs have been sold in the United States during that 11-year period. Adams Media Research DVD Data for 1997 to 2007 (document on file with author).

⁸² *Id.*

⁸³ Ben Fritz, *Sales of Digital Movies Surge*, WALL ST. J. (Jan. 7 2014), <http://www.wsj.com/articles/SB10001424052702304887104579306440621142958>.

⁸⁴ *Top-Selling DVDs in the United States 2015*, NUMBERS, <http://www.the-numbers.com/home-market/dvd-sales/2015> (last visited May 8, 2016).

⁸⁵ Solveig Singleton makes a persuasive case about this. *See* Solveig Singleton, *Copy Protection and Games: Lessons on DRM Debates and Development*, PROGRESS ON POINT (The Progress & Freedom Found., defunct), Feb. 2007, <http://www.pff.org/issues-pubs/pops/pop14.2gamecopyprotectDRM.pdf>.

At the turn of the new millennium, the music industry experimented with different types of DRM added to the CD format. “Experiment” is a key concept here, as different companies tried different technologies in different markets.⁸⁶ Tim Wu gave an apt description of the problem with CDs: “[A] successful locking strategy also requires intense cooperation between many actors—if you protect a song with ‘superlock,’ and my CD player doesn’t understand that, you’ve just created a dead product.”⁸⁷

Experiments with discrete-copy DRM on compact discs reached their nadir in 2005 when Sony BMG introduced millions of CDs with a system called “Extended Copy Protection.”⁸⁸ This DRM installed “rootkit” software on users’ players without notification that essentially allowed unnoticed access to the user’s computer.⁸⁹ The revelations of the rootkit installation led to hackers exploiting the new vulnerability on Microsoft computers,⁹⁰ and the ensuing uproar prompted action by several states Attorneys General and the filing of class action suits against Sony BMG.⁹¹ Sony BMG recalled many if not most of the affected CDs (offering replacement with non-DRM CDs), distributed different versions of a rootkit removal tool, and settled the lawsuits as it could.⁹²

⁸⁶ See, e.g., *NSyncDC Is Copy Protection “Experiment”*, NEW SCIENTIST (Oct. 2, 2001), <https://www.newscientist.com/article/dn1367-nsync-cd-is-copy-protection-experiment/> (describing Sony’s use of key2audio DRM with different protection settings in Germany and the U.S.); *BMG to Replace Antirip Natalie Imbruglia CDs*, REGISTER (Nov. 19, 2001), http://www.theregister.co.uk/2001/11/19/bmg_to_replace_antirip_natalie/ (describing Bertelsmann Music Group’s use of “Cactus Data Shield” DRM in Europe and failure to notify consumers that such CDs would not play in PC CD-ROM players); Jim Hu, *Warner Japan Adding CD Copy Protection*, CNET (Apr. 1, 2002), <http://www.cnet.com/news/warner-japan-adding-cd-copy-protection/#!> (describing “label’s ongoing trials to limit digital distribution of its songs” by introducing some CDs with DRM).

⁸⁷ Saul Hansell, *Bits Debate: Is Copy Protection Needed or Futile?*, N.Y. TIMES (Jan. 14, 2008), <http://bits.blogs.nytimes.com/2008/01/14/bits-debate-is-copy-protection-needed-or-futile/> (remarks of Tim Wu).

⁸⁸ *Sony BMG Litigation Info*, ELECTRONIC FRONTIER FOUND., <https://www EFF.org/cases/sony-bmg-litigation-info> (last visited May 8, 2016).

⁸⁹ See Mark Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far*, MARK’S BLOG (Oct. 31, 2005), <https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/> (describing how the Extended Copy Protection software was not described in the Sony end user license agreement (EULA) and how the software seemed to avoid detection, a characteristic of “rootkits”); see *Sony BMG Litigation Info*, *supra* note 90. (“Security researchers have shown that the XCP technology was designed to have many of the qualities of a ‘rootkit.’ It was written with the intent of concealing its presence and operation from the owner of the computer and once installed it degrades the performance of the machine opens new security vulnerabilities and installs updates through an Internet connection to Sony BMG’s servers.”).

⁹⁰ See, e.g., *World of Warcraft Hackers Using Sony BMG Rootkit*, REGISTER (Nov. 4, 2005), http://www.theregister.co.uk/2005/11/04/secfocus_wow_bot/.

⁹¹ *Sony Sued Over Copy-protected CDs*, BBC NEWS (Nov. 10, 2005), <http://news.bbc.co.uk/2/hi/technology/4424254.stm>.

⁹² Robert McMillan, *Sony Rootkit Settlement with US States Reaches \$5.75M*, NETWORKWORLD (Dec. 21, 2006), <http://www.networkworld.com/article/2302377/lan-wan/sony-rootkit-settlement-with->

The Sony BMG rootkit story may have been the contingent event that ended the music industry's experimentation with discrete-copy DRM. By 2007, more and more people working in digital music had concluded that discrete-copy DRM for sound recordings was not working. Steve Job's public opposition in February of that year probably shifted the tide definitively against DRM in the music space.⁹³

Despite all this, when academics make claims about "public opinion," we must be careful to make sure we are actually speaking about the public, not just self-appointed voices in the blogosphere or op-ed pages. In the case of digital music, even after the Sony BMG debacle, the evidence is mixed. One of the most interesting empirical studies in this area found evidence that TPM suppressed sales, but not necessarily because consumers were making choices based on the presence or absence of digital locks on content.⁹⁴ A study of over 5,900 albums released between 1992 and 2012 from over 600 artists "found that the removal of DRM from popular records had an insignificant impact on sales, while records that sold less than 25,000 copies saw a 30% increase in sales and records that sold less than 100,000 a 24% increase."⁹⁵ The study's author posited that this effect came not from consumer dislike of DRM, but because "DRM removal facilitates sharing of music from unpopular artists that otherwise would not have occurred, which can subsequently lead to the purchase of other music by the unpopular artist."⁹⁶ On the other hand, some surveys showed consumer dislike of DRM,⁹⁷ and the individual decisions of record labels to move away from DRM, particularly the most restrictive kind, seems to have been motivated by their own understanding of public preferences—how much that was from actual consumer experience and how much from blogosphere commentary is unclear.

Why did the music industry's experience with DRM go so badly compared to the DVD and videogame console industries'? Perhaps the answer lies in contingent patterns of technology distribution and, from that, consumer expectations. DVDs were introduced to consumers on a widely-

us-states-reaches--5-75m.html; Paul Taylor, *Sony BGM Bows to Pressure*, FIN. TIMES (Nov. 16, 2005), <http://www.ft.com/cms/s/2/e9e41f72-56f4-11da-b98c-0000e25118c.html#axzz40GagUEvT>.

⁹³ Dan Costa, *DRM Is Dead*, PC MAG. (Mar. 14, 2007), <http://www.pcmag.com/article2/0,2817,2102947,00.asp> (describing public opposition to music DRM by Jobs as well as Real-Networks' CEO, Rob Glazer, and Yahoo! Music's Dave Goldberg).

⁹⁴ Laurina Zhang, *Intellectual Property Strategy and the Long Tail: Evidence from the Recorded Music Industry 18-19* (Oct. 27, 2014) (unpublished manuscript), <http://ssrn.com/abstract=2515581>.

⁹⁵ Andrew Flanagan, *DRM Was a Bad Move: Sales Found to Increase 10% After Dropping the Chains (Study)*, BILLBOARD (Dec. 2, 2013), <http://www.billboard.com/biz/articles/news/digital-and-mobile/5812288/drm-was-a-bad-move-sales-found-to-increase-10-after>.

⁹⁶ Zhang, *supra* note 94, at 28.

⁹⁷ Ken Fisher, *Survey Says: Only DRM-free Music Is Worth Paying For*, ARSTECHNICA.COM (Aug. 5, 2007), <http://arstechnica.com/tech-policy/2007/08/survey-says-only-drm-free-music-is-worth-paying-for/> (describing survey of music consumers in the UK).

licensed, unitary technology platform with the DRM already built-in. Consumers who decided to switch from VHS to DVD could play a DVD from any movie studio on a DVD player from any electronics manufacturer. While videogame manufacturers did not offer consumers the same kind of unitary technology platform, the consumer purchasing a PlayStation, Xbox, or Wii knew/knows he is entering a “walled garden” technology.⁹⁸

The CD had also been introduced to consumers on a widely licensed, unitary technology platform in the 1980s, but one that did not have any DRM. Through the 1990s, the CD platform moved from dedicated CD players to general personal computers. By the time that record companies tried to introduce DRM-protected CDs, backward compatibility problems with all the CD-playing platforms were virtually inevitable.

This same compatibility problem has plagued some videogame discs, with the usual bad press for DRM,⁹⁹ but it seems clear that the problem for the music industry was that *limits* on where and when a digital music file could play—whether a CD or a download—defied established consumer expectations about *interoperability*, expectations that did not exist in the audiovisual and videogame space.

3. The Quietly Continued Story of “Discrete Copy” TPM

In a less discussed type of discrete-copy DRM, the consumer obtains a copy of a work that has a limited “shelf-life” for the copy, i.e., the copy “expires” either after a certain amount of time or after a subscription is ended. Some early special DVD formats experimented with such “expiration DRM,” perhaps the most fascinating being the “Flexplay” or “EZ-D” DVD format. Consumers purchased Flexplay discs in vacuum-sealed packages. A Flexplay disc could be played on a standard DVD player, but the digital

⁹⁸ The claustrophobia of the walls being lessened by independent game producers working to make their content available on the different platforms. Vlad Savov, *Microsoft Is Turning the PC into a Walled Garden and ‘We Must Fight It,’ Says Tim Sweeney*, VERGE (Mar. 4, 2016), <http://www.theverge.com/2016/3/4/11160104/tim-sweeney-microsoft-walled-garden-criticism>.

⁹⁹ For example, Microsoft’s Windows 10 has disabled and just won’t recognize videogame discs with “Safedisc” and Securom” DRM because of a security hole created by these DRM systems. Stang-Bit, *Securom in My EA Games in Origin in Windows10 Not Compatible What Now*, EA ANSWERS HQ (Sept. 7, 2015, 5:19 AM), <http://answers.ea.com/t5/Origin/Securom-in-my-EA-games-in-Origin-in-Windows10-not-Compatible/td-p/4771181>. One blogger reacted to this EA customer’s question by saying, “I wouldn’t blame Windows 10 for this, but it’s another example of the harm done by restrictive or draconian DRM.” yahel_1, *You Need to Read This*, Response to *Securom in My EA Games in Origin in Windows10 Not Compatible What Now*, EA ANSWERS HQ (Sept. 9, 2015, 11:00 AM), <http://answers.ea.com/t5/Origin/Securom-in-my-EA-games-in-Origin-in-Windows10-not-Compatible/td-p/4771181/page/2>.

encoding degraded a few days after opening because of an oxygen-reactive dye used in disc manufacturing.¹⁰⁰

Nowadays, “shelf-life” DRM is fairly familiar—with ebook lending from libraries,¹⁰¹ twenty-four- or forty-eight-hour video-on-demand downloads, and “subscription dependent” downloads, exemplified by the music files Spotify allows a subscriber to keep on her own device.¹⁰² The Spotify model is not unique; when a *subscription-based* streaming service allows the subscriber to keep a discrete copy of a provided work, the copy is typically “tethered” to the subscription through DRM, meaning that if the consumer ends the subscription the discrete copy is disabled or deleted.

B. *The Calmer World of Passwords, Firewalls, and Streaming Platforms*

Meanwhile, another kind of DRM—what we can call “platform DRM”—has succeeded both quietly and mightily.

Again, we can think of platform DRM as being either § 1201(a) access DRM, § 1201(b) “rights” DRM, or both. We obviously have a § 1201(a) access control when content is delivered only after the user has supplied a valid password/key, requesting either specific content or *participation* in some content-driven experience. As noted earlier, Westlaw and LEXIS presented this DRM model long ago, complete with the realization of the

¹⁰⁰ See Sarah N. Lynch, *This DVD Will Self-Destruct*, TIME (July 1, 2008), <http://content.time.com/time/business/article/0,8599,1817828,00.html>. With FlexPlay, the DRM is not something added “on top of” the content; it is a design characteristic built *into* the content’s media—like newspapers having cheap ink and paper stock that quickly goes yellow. But unlike newspaper stock, FlexPlay almost certainly counts as DRM designed to limit a consumer’s access to a work: if one applied a chemical to retard the leuco-dye oxidation in a FlexPlay disc, one would presumably violate 17 U.S.C. § 1201(a)(1).

¹⁰¹ More than 30,000 libraries in 40 countries “lend” ebooks through Overdrive.com. OVERDRIVE, <https://www.overdrive.com/> (last visited May 8, 2016). With these DRM ebooks, “[t]itles you’ve borrowed from the library will automatically be returned at the end of their lending periods,” meaning they are deleted from the library patron’s device automatically. *How to Return a Downloaded Title Using OverDrive for Android*, OVERDRIVE, <http://help.overdrive.com/customer/en/portal/articles/1482571-how-to-return-a-downloaded-title-using-overdrive-for-android> (last visited May 8, 2016).

¹⁰² See *Go Premium. Be Happy*, SPOTIFY, <https://www.spotify.com/us/premium/> (last visited May 8, 2016) (stating that Spotify’s “Premium” service allows the customer to “download music & listen offline”). The downloaded music files have a 30-day shelf life and the Spotify subscriber “need[s] to go online within the app at least once every 30 days” to “ensure [her] subscription is still active.” *Learn more/General Questions: How Long Can I Save Offline Music on My Device?*, SPOTIFY, <https://support.spotify.com/us/learn-more/faq/#!/article/how-long-can-i-cache-offline-content> (last visited May 8, 2016). Each time the Spotify Premium subscriber goes online, “the remaining time” on the downloads “is set back to 30 days.” *Id.* This kind of subscription-tethered download has also been used with video games. See *Atari, Inc. v. Games, Inc.*, No. 04 Civ. 3723(JSR), 2005 WL 612711, at *1 (S.D.N.Y. 2005) (“[D]ownloaded versions [of games] are sold as part of time-limited subscriptions services, [so] their files are encrypted such that the user cannot start a game without running a launcher program, which authenticates the user’s license over the Internet.”).

often-mentioned concern of public domain materials made inaccessible because of digital locks. Many major newspapers today use a related “freemium” business model in that some content is freely available but consumers must purchase access to more desirable, often more timely content.¹⁰³

Essentially, any password-protected subscription service qualifies as platform DRM. Of course, such password/firewall protection systems are ubiquitous in computer networks,¹⁰⁴ and it is worth pointing out that many systems were already protected pre-DMCA by the Computer Fraud and Abuse Act of 1986¹⁰⁵ (“CFAA”). Breach of a firewall/password DRM to access content on the servers of a service like LEXIS, FT.com, or washingtonpost.com will almost certainly mean “intentionally access[ing] a computer without authorization or exceed[ing] authorized access” so as to obtain “information from any protected computer.”¹⁰⁶ Nonetheless, password/firewall systems are definitely within the intended scope of

¹⁰³ See ‘Paywalls’ Become the Norm at US Newspapers: Survey, PHYS.ORG (Feb. 29, 2016), <http://phys.org/news/2016-02-paywalls-norm-newspapers-survey.html> (“The ‘paywall’ model varies at the publications, the survey found: 62 newspapers used a ‘metered’ system that allows visitors to read a specified number of articles for free, while 12 used a ‘freemium’ model that offers some kinds of content for free and others only to subscribers.”); see also Ryan Chittum, *The NYT Paywall Is Out of the Gate Fast*, COLUM. JOURNALISM REV. (July 22, 2011), http://www.cjr.org/the_audit/the_nyt_paywall_is_out_of_the.php (describing the New York Times paywall).

¹⁰⁴ See generally WALLACE WANG, STEAL THIS COMPUTER BOOK 4.0: WHAT THEY WON’T TELL YOU ABOUT THE INTERNET 115-35 (2006).

¹⁰⁵ Pub. L. No. 99-474, 100 Stat. 1213 (current version at 18 U.S.C. § 1030 (2012)).

¹⁰⁶ 18 U.S.C. § 1030(a)(2)(C). As summarized by one commentator:

For ordinary civil liability purposes, the CFAA applies to anyone who: (1) “intentionally accesses a computer without authorization or exceeds authorized access [and thereby obtains] information from any protected computer if the computer involved an interstate or foreign communication;” (2) “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;” (3) “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;” (4) “intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;” or (5) “by conduct described in . . . subparagraph (A) [(2)-(4) above], caused (or, in the case of an attempted offense, would, if completed, have caused—(i) loss to 1 or more persons during any 1-year period aggregating at least \$5,000 in value.”

Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 479-80 (2003) (footnotes omitted) (quoting 18 U.S.C. § 1030(a)(2), (a)(5)(A), (a)(5)(B)(i) (2000)). In *I.M.S. Inquiry Management Systems Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d 521 (S.D.N.Y. 2004), the defendant had used a legitimate account name and password to access a website and extract information beyond what was contractually permitted. *Id.* at 524-27. The court found that the plaintiff had adequately stated a claim under the CFAA and that the password system was an access control protected by the DMCA, but the court also found that *unauthorized* use of a *legitimate* password was not circumvention under § 1201(a). *Id.* at 525-26, 531-32. In *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D. Me. 2003), the court found that circumventing an “encrypted, password-protected virtual private network” violated § 1201(a), *id.* at 349-50, but failure to allege the requisite damage caused the CFAA claim to fail. *Id.* at 348-349.

§ 1201¹⁰⁷—indeed, it is hard to think of a cleaner, simpler example of a § 1201(a) “access” control.

Once the consumer has access to a site that is providing content, it is not uncommon that DRM will control how the content is delivered to the consumer and what the consumer can do with that content. The focus of the discussion here is websites and services that *stream* audiovisual content. While a password protected service like Westlaw or *The Wall Street Journal* online allows the subscriber to download entire documents, with a streaming service for audio or audiovisual works, only a very small portion of the overall work is displayed on a subscriber’s device at any one time. After the stream, “no trace of the [work] is left on the consumer’s computer, unless the content owner has permitted the consumer to download the file.”¹⁰⁸ Some of these web services provide unrestricted access. YouTube is the dominant player in this type of service while other services like Vimeo and Dailymotion also have substantial user bases.

Other audiovisual streaming services like Netflix, Hulu, Amazon Prime, and video-on-demand services are subscription based, whether they are delivered via the Internet or cable television systems. All such subscription services are encrypted, meaning that “access” to the streamed content is protected by § 1201(a) technological measures. But after a transmission to the player device is decrypted, the same or different DRM measures may provide protection that would fall under § 1201(b).

For example, when a service like Netflix provides an encrypted stream to a tablet or smartphone, the tablet or smartphone decrypts and the content is accessible to the consumer, but the tablet or smartphone will be configured to limit further transmission of the content. With a content delivery system to anything that would count as a “set top box” separate from the television, the set top box will decrypt the transmission and, depending on the device and service, may allow the consumer to retain a copy for personal viewing. Although a § 106 reproduction has occurred, the set top box is almost certainly configured to prevent or limit distribution of further copies (as to other devices in the home). Thus, § 1201(b) protection still occurs. For the consumer to view the show, the set top box will re-encrypt the signal in “high definition content protection” (“HDCP”), an encrypted format that serves as a common, licensed platform for televisions (hence called a “link” DRM). If the television complies with the HDCP license, it lacks the capacity to capture and store the signal, hence the HDCP encryption serves as both a § 1201(a) and § 1201(b) digital lock.

¹⁰⁷ H.R. REP. NO. 105-551, at 37 (1998) (“Many such technological protection measures are in effect today: these include the use of ‘password codes’ to control authorized access to computer programs, for example, or encryption or scrambling of cable programming, videocassettes, and CD-ROMs.”); *see also* S. REP. NO. 105-190, at 16 (1998).

¹⁰⁸ *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *1 (W.D. Wash. Jan. 18, 2000).

On the Internet, regardless of whether or not § 1201(a) gatekeepers guard access to the audiovisual stream, all or almost all of these streaming services employ *some* technological measures to *limit* user's ability to convert the audiovisual *stream* into a *download*. This DRM prevents the exercise of copyright's § 106 right of reproduction. Indeed, maintaining the difference between a stream and a download is basic to all these business models.¹⁰⁹ Different operating systems have different dominant § 1201(b) technological measures to prevent reproduction: Microsoft's "Playready," Apple's "Fairplay," and the "Widevine" system for Google's Android operating system.¹¹⁰ Again, these DRM systems offer functionality that can fall under § 1201(a) or § 1201(b) *or both*; the same is true with other DRM systems, such as the Open Mobile Alliance ("OMA") system for mobile devices¹¹¹ and the "Marlin" DRM from a consortium of electronic companies including Sony, Samsung, and Philips.¹¹²

In the case of a YouTube stream, there is no § 1201(a) access gatekeeper and the stream is made available in the HTML5 video player format, meaning a user may capture the stream. This has given rise to different "conversion" websites, including those that extract an audio .mp3 file from a music video available on YouTube. As one report described one of the sites, "What [a conversion site] does is straightforward. At one end a user feeds the site with a YouTube URL and after a couple of minutes the site spits out a standalone MP3 file, perfect for ripping the audio from pop videos."¹¹³ In 2012, YouTube went after some of these sites, sending them cease-and-desist letters for violation of YouTube's terms of service¹¹⁴ and then blocking the servers of at least one conversion site.¹¹⁵

In 2000, RealNetworks took a similar defendant to court, with the court finding the defendant's "Streambox VCR" to be "primarily, if not exclusively, designed to circumvent the access control and copy protection measures that RealNetworks afford[ed] to copyright owners" through its

¹⁰⁹ Or, as one court has said, "In the digital era, the difference between streaming and downloading is of critical importance." *Id.* at *2.

¹¹⁰ To clarify: while these specific DRM are associated with the dominant operating system providers, with mobile devices the DRM is app-specific, so one might have an app using Playready while running on an Android device. My thanks to Mitch Singer for this point.

¹¹¹ The OMA consortium includes a large number of mobile phone manufacturers, mobile phone network operators, and technology companies. *Frequently Asked Questions*, OPEN MOBILE ALLIANCE, <http://openmobilealliance.org/about-oma/frequently-asked-questions/> (last visited May 8, 2016).

¹¹² *Marlin History & Founders*, MARLIN, <http://www.marlin-community.com/about> (last visited May 8, 2016).

¹¹³ Enigmax, *Google Threatens to Sue Huge YouTube mp3 Conversion Site*, TORRENTFREAK.COM (June 19, 2012), <https://torrentfreak.com/google-threatens-to-sue-huge-youtube-mp3-conversion-site-120619/>.

¹¹⁴ *Id.*

¹¹⁵ *Id.* ("Google has just blocked all of YouTube-MP3's servers from accessing YouTube so currently the site has no MP3 download service to offer or indeed withdraw."). The blocking of YouTube-MP3.com has either stopped or has proved ineffective (or both).

“RealPlayer” device.¹¹⁶ But aside from that case, there has been no or almost no litigation about streaming platform DRM.

Of course, the anti-circumvention standards of § 1201 have not stopped all attempts to break the digital locks protecting streamed content. Because a single streaming service may be on multiple downstream platforms, the “digital locks” need to be robust at each level and with each delivery platform. Netflix, for example, is available at Netflix.com, Netflix apps, Xbox, PlayStation, Roku, AppleTV, etc. Netflix’s own stream is protected by PlayReady (and probably other DRM), but the receiving device itself must comply with DRM licensing requirements on playing, any storage, and/or onward transmission (re-encrypting with a “link” DRM). In the fall of 2015, new breaches of the High-Bandwidth Digital Copy Protection (HDCP) affected content carried on Netflix and Amazon, but this probably means the breaches occurred downstream after the encrypted content had been handed off to a licensed device.

And § 1201 hardly answers all the interesting cases that may arise. For example, as a matter of § 1201 analysis, as long as YouTube does not employ access controls, the open HTML5 format of its streams means that YouTube conversion sites would not initially violate § 1201 although these activities would still be an unauthorized reproduction and distribution of the captured .mp3 file. But we might have an interesting § 1201 problem if, when YouTube took actions to block a conversion site, the conversion site attempted evasive action to regain access. One company configuring its own servers to block communications from another company’s servers would arguably be a § 1201(a) technical measure.

Another example of the frontiers of § 1201 might be the ways that streaming sites attempt to limit their services to geographic territories where they have the necessary licensing and authorization. Hulu, for example, operates only in the United States and Japan, while “Netflix is only available in a few dozen countries, all of which have a different content library.”¹¹⁷ This business plan obliges them to “geo-block” IP addresses known to be outside the licensed territories,¹¹⁸ prompting some consumers to turn to Virtual Private Network (“VPN”) IP addresses. This circumven-

¹¹⁶ RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000).

¹¹⁷ Ernesto, *Netflix Cracks Down on VPN and Proxy “Pirates”*, TORRENTFREAK.COM (Jan. 3, 2015), <https://torrentfreak.com/netflix-cracks-down-on-vpn-and-proxy-pirates-150103/> [hereinafter Ernesto, *Netflix Cracks Down*].

¹¹⁸ Geo blocking is “[t]he practice of preventing users from viewing Web sites and downloading applications and media based on location. Used by countries to block foreign material as well as by movie and TV studios to restrict viewing to specific regions, geo-blocking is accomplished by excluding targeted Internet addresses.” *Geo-blocked Definition*, PC MAG., <http://www.pcmag.com/encyclopedia/term/61864/geo-blocked> (last visited May 8, 2016). For a discussion of evasion of geo-blocking and § 1201, see Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 619-620 (2012).

tion, in turn, has triggered Netflix and Hulu to block known VPN IP addresses.¹¹⁹ Although we have no such litigations, a consumer's intentional use of a VPN to avoid a streaming service's geo-blocking would presumably be a § 1201(a)(1) violation, although the consumer using VPNs would presumably be outside the jurisdiction of American courts.

CONCLUSION

After the major record labels one by one ditched DRM on CDs, the move to DRM-free digital files at iTunes in early 2009 seemed to effectively eliminate discrete-copy DRM *in the music industry*. That chain of events created an impression that “DRM is dead.”¹²⁰ But wiser observers knew that this conclusion was never true. Discrete-copy DRM remained alive and well in the videogame and audiovisual sectors; discrete-copy DRM made and makes it possible for libraries to “lend” ebooks and for Spotify to allow its subscriber devices to have copies of sound recordings that can play when the device is not connected to the Internet.

More importantly, it now appears that consumers will increasingly experience copyrighted content through streaming platforms—the digital networked counterparts to traditional cinemas, broadcast television, and time-shifted enjoyment of the same. These streaming platforms—Amazon Prime, AppleTV, GooglePlay, Hulu, Netflix, Hulu and all the iROKOtv platforms that may arise—depend on *general* consumer acceptance of the digital locks that separate streaming business models from download business models. For Nollywood, the digitally locked world of making works available through transmission—whether scrambled satellite broadcasts or encrypted Netflix streams—looks like a hopeful way to generate revenue that will allow audiovisual production values to improve and people working in that industry to enjoy better wages. Anti-circumvention laws like § 1201 create the background legal regime to protect those digital locks. So, as a *Wired* magazine commentator noted in 2008, “DRM Is Dead; Long Live DRM.”¹²¹

¹¹⁹ Ernesto, *Hulu Blocks VPN Users over Piracy Concerns*, TORRENTFREAK.COM (Apr. 25, 2014), <https://torrentfreak.com/hulu-blocks-vpn-users-over-piracy-concerns-140425/>; Ernesto, *Netflix Cracks Down*, *supra* note 117.

¹²⁰ Matt Buchanan, *DRM Officially Dead: Last Major Label Sony BMG Plans to Finally Drop DRM*, GIZMODO.COM (Jan. 4, 2008), <http://gizmodo.com/340598/drm-officially-dead-last-major-label-sony-bmg-plans-to-finally-drop-drm>; Costa, *supra* note 93; David Kravets, *DRM Is Dead, but Watermarks Rise from Its Ashes*, ELECTRONIC FRONTIER FOUND. (Jan. 11, 2008), <https://www.eff.org/press/mentions/2008/1/11-0>.

¹²¹ Ryan Singel, *DRM Is Dead; Long Live DRM*, WIRED (Jan. 14, 2008), <http://www.wired.com/2008/01/drm-is-dead-lon/>.