Hearing Before the United States Senate Judiciary Committee
Subcommittee on Intellectual Property

Copyright Law in Foreign Jurisdictions: How are other countries handling digital piracy?

10 March 2020

Statement of Professor Justin Hughes
Loyola Marymount University
Los Angeles, California

Introduction

In the early years of the widely-available internet access, governments settled on a compromise that an internet service provider would not be liable for copyright infringements caused by its users as long as the intermediary acted promptly to disable the information when so requested. With the 1998 Digital Millennium Copyright Act (DMCA), the United States was truly the leader in the development of that consensus. As several witnesses said at your February hearing, the DMCA combined legal protection of "digital locks" used to protect copyrighted works [17 USC § 1201] with a set of safe harbors for internet service providers (ISPs) that would shield an ISP from copyright liability as long as it was not aware of the copyright infringement and acted "expeditiously" to disable or block the infringement once it received notice from the copyright owner [17 USC § 512]. In rough form, this compromise on ISP liability was embraced fairly quickly by the international community – in the European Union, Japan, China, Australia, Singapore, and many other jurisdictions.[1]

[1] For a near contemporaneous description of some of this, see Justin Hughes, *The Internet and the Persistence of Law*, 44 BOSTON COLLEGE L. REV. 359 (2003).

Unlike some of your witnesses in February, I do not think that § 512 "was obsolete on arrival"[2] and I do not think that § 1201 is "broken"[3] or "has not lived up to its promise."[4] In fact, I think that both branches of the DMCA have proved surprisingly robust and resilient.

Nonetheless, it is true that technology and new business models have changed the internet landscape significantly from what Congress and other national legislatures saw in the late 1990s and early 2000s. In the years since 1998, courts around the world have taken on the job of adapting legislation written for a "dumb" internet to increasingly intelligent platforms and increasingly sophisticated business models, some designed to abide by the law and some designed to test it. Today, there are both visible cracks and visible loopholes in what has been a very robust system.

Last year, in passing the 2019 Digital Single Market Directive,[5] the European Union effectively broke rank from the old consensus limiting the copyright infringement liability of *all* internet platforms and systems. The EU has now chosen – I think quite reasonably – to put more responsibility for copyright enforcement on the shoulders of *some* multi-billion dollar platforms. Today I hope to talk to you about the DSM Directive as well as different copyright enforcement efforts in other jurisdictions, how those compare to the DMCA, offer some responses to things said by witnesses in your February hearing, and suggest how the subcommittee might undertake thoughtful, careful amendment of the DMCA in a way that could achieve consensus among the many stakeholders.

HOW THE §512 SAFE HARBORS FUNCTION TODAY

As you know, §512 establishes – in subsections (a) through (d) respectively – distinct safe harbors for transmission ISPs, caching ISPs, hosting ISPs, and search engines. The last three of these are subject to a knowledge standard, including the "notice and takedown" system set out in §512(c). If a hosting, caching, of "information location tool" ISP fails to "expeditiously" disable access to alleged infringing material identified in a notice, the ISP loses the protection of the safe harbor and can be laible for the infringement. This approach was repeated in rough form in the European Union's 2000 E-Commerce Directive[6] as well as laws in Australia, China, India, Japan, Singapore, and other countries.

---

[2] *The Digital Millennium Copyright Act at 22: What is it, why was it enacted, and where are we now,* Hearing before the Senate Judiciary Committee Subcommittee on Intellectual Property, 116th Cong. (February 11, 2020) (Statement of Professor Mark Schultz at 10).

[3] *The Digital Millennium Copyright Act at 22: What is it, why was it enacted, and where are we now,* Hearing before the Senate Judiciary Committee Subcommittee on Intellectual Property, 116th Cong. (February 11, 2020) (Statement of Professor Rebecca Tushnet at 2) [hereinafter Tushnet Statement].

[4] *The Digital Millennium Copyright Act at 22: What is it, why was it enacted, and where are we now,* Hearing before the Senate Judiciary Committee Subcommittee on Intellectual Property, 116th Cong. (February 11, 2020) (Statement of Professor Jessica Litman at 5) [hereinafter Litman Statement].

[5] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, available at https://eur-lex.europa.eu/eli/dir/2019/790/oj [hereinafter "DSM Directive"].

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular, Electronic Commerce, in the Internal market, 2000 O.J. (L 178), available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031. The E-Commerce Directive does not expressly have "notice and takedown" provisions, but since the ISP must act "expeditiously" once it has knowledge of the alleged infringement, copyright owners can trigger such knowledge through notices. Some EU jurisdictions developed specific notice and takedown provisions. In France, Article 6.I.2 of the Loi pour la Confiance dans

Your February hearing gave you some varied pictures of the §512 notice and take down regime because that regime functions in different ways for different ISPs. In an extensive study of the §512 system, Jennifer Urban, Joe Karaganis, and Brianna L. Schofield divided ISPs into those working under a "classic" system – that is, as §512 was envisioned in 1998 – and those working within a "DMCA Auto" system.[7] Professor Rebecca Tushnet has already given a good description of her experience with a non–profit hosting site working under the "classic system" involving substantive human review of infrequently-received takedown notices. That remains a large part of the overall §512 system, but it is important for you to appreciate the scale and scope of "auto" DMCA before we talk about international developments.

When it comes to major platforms, today content owners employ automated systems to detect copyright infringements. These automated systems on the content owners side then send that information – as digitized §512 "notices" – to automated systems on the ISP side. The scope of this unseen activity is epic. According to the Google Transparency Report, as of Sunday, March 8, 2020, Google Search had received notices to delist from search results 4,517,495,427 URLs from over 200,000 copyright owners.[8] Microsoft's Bing search engine summarizes data a little differently, but reports having received 13,380,111 notices involving 81,869,212 URLs during the period January to June 2019.[9] Microsoft reports accepting the notice and disabling the URL from search results in 99.67% of the requests.[10]

In addition to this §512 notices and takedown system being highly automated, in the case of §512(d) – notice and take down for information location tools – the global dominance of the US-based search engines[11] appears to have converted §512(d) into an important copyright enforcement tool *outside* the United States. Of the organizations filing takedown notices to Google Search, the second most active organization is the BPI (British Recorded Music Industry) Ltd with .eu and .pl domain names being among its top targets for "noticed" URLs.[12] The fourth and fifth most active notice filers are trade associations representing the Mexican and Brazilian music industry, with 262,318,538 and 249,407,601 targeted URLs respectively.[13]

Fortunately, the wording of the DMCA is general enough that this system of automated notice and takedown can reasonably fit within the statutory parameters.

---

l'Economie Numérique (LCEN) provides that an ISP "cannot incur civil liability as a result of the activities or information stored at the request of a recipient of those services if they were not in fact aware of the illegality or circumstances that reveal this character or if, from the moment they have had this knowledge, they have acted promptly to remove this data or make it impossible to access it." Article 6.I.5 then establishes a rebuttable presumption of knowledge on the part of the ISP when the ISP receives a "notice" that meets requirements set out in the provision. Loi pour la Confiance dans l'Economie Numérique (LCEN) [Law on Confidence in the Digital Economy], No. 2004-575 of June 21, 2004, available at https://wipolex.wipo.int/en/legislation/details/12761.

7 JENNIFER M. URBAN, JOE KARAGANIS & BRIANNA L. SCHOFIELD, NOTICE AND TAKEDOWN IN EVERYDAY PRACTICE, Version 2 at 28 (March 2017).

8 *Google Transparency Report*, available at https://transparencyreport.google.com/copyright/overview

9 MICROSOFT CORPORATION, CONTENT REMOVAL REQUESTS REPORT, available at https://www.microsoft.com/en-us/corporate-responsibility/crrr/. Microsoft reported receiving 13,379,128 requests related to 97,221, 136 URLs for the parallel period in 2018. All these numbers do not include takedown notices that Microsoft received in relation to the Bing image or video search functions, from Bing Ads, or from Outlook and Skype. *Id.*

10 *Id.*

11 Except in China.

12 *Google Transparency Report, Content delistings due to copyright, Reporting Organization View*, available at https://transparencyreport.google.com/copyright/reporters/1847.

13 *Google Transparency Report*, available at https://transparencyreport.google.com/copyright/overview

ARTICLE 17 OF THE EU "DIGITAL SINGLE MARKET" DIRECTIVE

On 15 April 2019, the European Council gave final approval to the "Single Digital Market Directive" (the SDM Directive), the most comprehensive revision of European copyright law since the 2001 Information Society Directive harmonized basic copyright right, established protection of technological measures, and set out a framework for copyright exceptions and limitations in European national copyright laws.[14] Much has been written about the intense political push from all sides on the SDM directive. Content owners and creative professionals appear to have engaged in more traditional lobbying with some more modern public relations efforts.[15] American tech companies and related digerati[16] used the same traditional methods, but also tried to rally EU citizens against the Directive through "tools of automated consensus generation,"[17] that probably angered European politicians more than anything else.[18]

The SDM Directive offers new, harmonized exceptions and limitations to copyright; provides a framework for data mining which is critical to "big data" and much of AI research; and provides some new protections for authors, artists, and other creative professionals. But its most debated provisions are what became Articles 15 and 17. Article 15 requires news aggregators like Google or Yahoo! News to pay remuneration for excerpts of news stories shown online, anything other than "very short extracts." Whether such payments can meaningfully improve the finances of newspapers

---

[14] 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, 2001 O.J. (L 167) 10.

[15] See, e.g., video from the UK's Performing Rights Society (PRS), available at https://www.facebook.com/PRSforMusic/videos/vb.50991611802/1591946710948951/?type=2&theater.

[16] Based on various reports, entities as lobbying against the directive included the Computer & Communications Industry Association (and, by implication, its member companies), the Electronic Frontier Foundation, Facebook, Google, Mozilla, and the Open Society Foundation.

[17] Andrew Orlowski, *Article 13 pits Big Tech and bots against European creatives*, THE REGISTER, 12 September 2018 (describing automated email and phone call systems used by organizations linked to Google, Mozilla), available at https://www.theregister.co.uk/2018/09/12/youtube_article13_special_report/?page=2; Von Volker Rieck, *Anatomy of a Political Hacking,* FRANKFURTER ALLEGMEINE, 4 September 2018 (concluding that efforts by American tech companies included six million bot-generated emails sent to European Parliament Members from shadowy web sites that amounted to "clandestine attacks on [EU] democratic institutions"), available at https://www.faz.net/aktuell/feuilleton/medien/eu-and-copyright-anatomy-of-a-political-hacking-15771185.html?printPagedArticle=true#pageIndex_0; David Ruvics, *Google Funds Website that Spams for its Causes,* THE TIMES (of London), August 6, 2018, available at https://www.thetimes.co.uk/article/google-funds-activist-site-that-pushes-its-views-rg2g5cr6t

[18] In an uncharacteristic – and eventually disabled – blogpost the European Commission railed against what it colorfully described as Google's deceptive campaign to get "ordinary people [to] side with the fire breathing dragon against the knight with a blue and yellow shield"; more plainly, the Commission wrote that there was ample evidence from respected sources that 'Big Technology' has even "'created' grassroots campaigns against the Copyright Directive in order to make it look and sound as if the EU is acting against the 'will of the people'." Daniel Sanchez, *European Commission Lambastes Copyright Directive Critics – Then Deletes the Post*, DIGITAL MUSIC NEWS, February 19, 2019, available at https://www.digitalmusicnews.com/2019/02/19/eu-commission-criticism-retraction/. *See also* Corporate Europe Observatory, *Copyright Directive: competing big business lobbies drowned out critical voices*, 10 December 2018 (Fall 2018 work on the Directive was "the continuation of the battle that took over the European Parliament this summer, where accusations of deceptive and unfair lobbying, including tactics like astroturfing and spambots, played a decisive role. The voices of civil society organisations, small platforms, libraries, academics, citizens and even the UN Special Rapporteur on Freedom of Opinion and Expression were the collateral damage of the dispute between competing big business lobbies.") available at https://corporateeurope.org/power-lobbies/2018/12/copyright-directive-how-competing-big-business-lobbies-drowned-out-critical.

remains to be seen, but if you believe serious journalism undergirds democratic societies, it seems like an experiment worth trying.

Article 17 is a much clearer break with the consensus that had emerged internationally after 1998 to limit the liability of ISPs. It establishes a different regime of responsibility and liability for a new sub-category of ISPs called "online content-sharing service providers" defined as "a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes."[19] On one side, the DSM Directive expressly excludes from this new category "not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms" and business-to-business cloud platforms;[20] start-ups below a certain size are also exempted from Article 17's requirements.[21] On the other side, Article 17 excludes "service providers the main purpose of which is to engage in or to facilitate copyright piracy."[22] The Directive's definitional components presumably applies the new regime to Dailymotion, Facebook, Instagram, Vimeo, and YouTube.[23]

A content-sharing platform publicly perform, but that would not change the DMCA

With this focused definition, Article 17 first provides that "an online content-sharing service provider *performs an act of communication to the public or an act of making available to the public* for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users."[24] The result – expressly confirmed in Article 17(3) – is to take Facebook and YouTube out of the safe harbor provided by Article 14 of the EU's 2000 Electronic Commerce Directive,[25] the equivalent of the §512(c) safe harbor for hosting sites. The

---

[19] DSM Directive at Article 2(6). The recitals to the Directive provide that "The definition of an online content-sharing service provider laid down in this Directive should target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences. The services covered by this Directive are services, the main or one of the main purposes of which is to store and enable users to upload and share a large amount of copyright- protected content with the purpose of obtaining profit therefrom, either directly or indirectly, by organising it and promoting it in order to attract a larger audience, including by categorising it and using targeted promotion within it." *Id* at Recital 62.

[20] DSM Directive at Article 2(6).

[21] DSM Directive at Article 17(6).

[22] DSM Directive at Recital 62.

[23] As one law firm blog notes, "In most cases, it should be self-evident whether or not storing and providing public access to large amounts of uploaded content is a main purpose or merely incidental to another main purpose" Toby Headdon, *Am I an 'Online Content Sharing Service Provider' under Article 17 (formerly Article 13) of the proposed Copyright Directive*, Bristows, April 10, 2019, available at https://www.bristows.com/news/am-i-an-online-content-sharing-service-provider-under-article-17-formerly-article-13-of-the-proposed-copyright-directive/.

[24] DSM Directive at Article 17(1).

[25] DSM Directive at Article 17(3) ("When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive, the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article.")

DSM Directive also "transfers" the act of communication or making available to the public from the individual who uploads the content to the "online content-sharing service provider"[26]

So, in American copyright terminology, the DSM Directive provides that Facebook or YouTube, not the uploader, "publicly performs" an audiovisual work each time it transmits that work to a consumer: Article 17(1) says that what YouTube does is no different than what Hulu, Spotify, or Netflix do. This shift may sound like a radical step, but it is not as strange as it may seem and, by itself, probably would not affect YouTube's protection under the DMCA safe harbors. I should explain each of these points.

First, as a matter of common sense, we now know that YouTube is a $15 billion annual business that has grown impressively in recent years;[27] it is as big or bigger than many of the corporate entities we would identify as big "media companies." While users upload almost all the content distributed by this particular media company, YouTube processes and converts those uploads into different technical formats as well as curates the overall uploaded library with recommendation algorithms that propose what the viewer should watch next. YouTube indexes all this content to produce a searchable library of audiovisual works; when the individual user finds a work she wants to see or hear, YouTube transmits that work to the individual at a time and place chosen by the individual user.

If some of that terminology sounds familiar, it should. In 2014, the Supreme Court decided *ABC v. Aereo*,[28] concluding that a platform which recorded television shows at a user's requests then transmitted the recorded shows back to the user when she wanted to view the recorded program was engaged in unauthorized "public performance" of the recorded television shows. Confronting the question whether "Aereo 'transmit . . . a performance' . . . or is it only the subscriber who transmits?"[29] the Court concluded that by providing an integrated service to its customers "Aereo is not just an equipment supplier and . . . Aereo 'perform[s].'"[30] The remaining issue was whether this activity was a § 106(4) "*public* performance." Reasoning that "an entity may transmit a performance through one or several transmissions, where the performance is of the same work," the Court also found that Aereo's activities constituted "public" performance of the recorded television shows.[31]

---

[26] Andrew Orlowski, *Ok, Google? Probably Not! Eu settles on wording for copyright reform legislation*, THE REGISTER, 14 February 2019 (quoting Axel Voss, the European Parliament member who shepherded the directive through the final "trilogue" process, "[w]e managed to ensure that the user of the platform would not be liable for uploading something because, legally speaking, that would be copyright infringement. We've moved the liability from the user to the platform") available at https://www.theregister.co.uk/2019/02/14/eu_copyright_reform_tweaks/

[27] *A Peek Inside YouTube's Money Machine*, Dealbook, N.Y. TIMES, February 4, 2020, available at https://www.nytimes.com/2020/02/04/business/dealbook/youtube-alphabet-revenue.html?auth=login-email&login=email. YouTube revenue was up 36% from the year before. Todd Spangler, *Alphabet Reports YouTube Ad Revenue for First Time, Video Service Generated $15.1 Billion in 2019*, VARIETY, February 3, 2020, available at https://variety.com/2020/digital/news/alphabet-youtube-ad-revenue-first-time-15-billion-2019-1203491155/#!.

[28] American Broadcasting Companies v. Aereo, 573 U.S. 431 (2014).

[29] *Id.* at 438.

[30] *Id.* at 444.

[31] *Id.* at 447. The Court correctly noted "[t]he Transmit Clause must permit this interpretation, for it provides that one may transmit a performance to the public 'whether the members of the public capable of receiving the performance … receive it … at the same time or at different times.' § 101. Were the words 'to transmit … a performance' limited to a single act of communication, members of the public could not receive the performance communicated 'at different times.'" *Id.*

One could draw some meaningful distinctions between Aereo and YouTube,[32] but it remains that much of the *Aereo* reasoning points to YouTube engaging in § 106(4) public performance of the works uploaded by YouTube users.

But that conclusion would not necessarily rob YouTube of the §512(c) safe harbor. At the time the DMCA was drafted Congress did not know whether courts would find ISPs liable for copyright infringement and, if so, whether as direct, contributory, or vicarious infringers. The DMCA's legislative history is clear: §512 (a)-(d) are also safe harbors against monetary damages for direct infringement.[33] Under the DMCA, the broadest reading of *Aereo* would not jeopardize YouTube's eligibility under the §512(c) safe harbor.

The license-or-filter requirement

But Article 17 goes further than saying Vimeo and YouTube publicly perform audio and audiovisual works the platforms stream to users. Article 17 makes the express decision that Article 14 of the E-Commerce Directive – the European counterpart to 512(c) – will no longer apply to these "online content-sharing service providers." Instead the online content-sharing service providers will be expected to obtain authorizations from copyright holders – "for instance by concluding a licensing agreement" – for all public performances of works.[34] If the platform does not have authorization, it will be liable for unauthorized exploitation of the copyrighted works unless

> ". . . the service providers demonstrate that they have:
>
> "(a) made best efforts to obtain an authorisation, and
>
> "(b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event
>
> "(c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites,

---

[32] For example, the majority seems to have been strongly motivated by "the many similarities between Aereo and cable companies, considered in light of Congress' basic purposes in amending the Copyright Act" to impose copyright liability on cable retransmitters. *Id.* at 444. YouTube does not have such "many similarities."

[33] DIGITAL MILLENNIUM COPYRIGHT ACT CONFERENCE REPORT, Report 105-796, 105th Congress, 2d Session, at 73 [Joint Explanatory Statement of the Committee of the Conference] ("The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement."); DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 REPORT TOGETHER WITH ADDITIONAL VIEWS, Report 105–551, Part 2, 105th Congress, 2d Session, at 43 ("*Subsection (c)–Information stored on service providers.*–Subsection (c) limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.")

[34] DSM Directive at Article 17(2).

> the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b)."[35]

Element "(b)" is widely understood to impose a filtering requirement on these platforms that will essentially be a "notice and stay down" system.[36] This "best efforts" obligation is set to "high industry standards of professional diligence" but is also subject to a proportionality test taking account of the platform's audience, the types of works involved, and "the availability of suitable and effective means and their cost for service providers."[37]

Article 17(7) also includes general language intended to ensure that when user-uploaded content should enjoy a copyright exception the content is not disabled or removed.[38] There is an on-going stakeholder dialogue which has recently turned to the problem of how to balance "ensur[ing] the unavailability" of unauthorized works with this protection of user quotation, criticism, and parody.[39] One group of European copyright academics has proposed a two-tier system in which "prima facie" infringements, i.e. an identical or equivalent matches to protected content, would be automatically blocked, while partial matches identified by an automated system would be flagged for human review before filtering.[40]

Separate from all these components of Article 17 and the rest of the DSM Directive, is imposing such responsibility good policy?

I agree with participants at the February hearing who felt that these sorts of obligations would simply be too onerous for many websites – and, of course, in the EU Article 17 seems likely to apply to relatively few websites. The DMCA notice and takedown system remains the best balance for websites that are using the law in the "classic" sense described in the Urban, Karaganis, and Schofield study.

The question is whether it is time to make some of the largest, most profitable platforms – lucrative platforms built upon "free" inputs from users – take on the kind of "notice and stay down"

---

[35] DSM Directive at Article 17(4).

[36] *See, e.g.* Marc Rees, *Directive Droit d'auteur : déjà une mission Hadopi-CNC-CSPLA sur la reconnaissance des contenus,* NEXTINPACT, March 28, 2019 (describing Article 17 as a notice and stay down system), available at https://www.nextinpact.com/news/107746-directive-droit-dauteur-deja-mission-hadopi-cnc-cspla-sur-reconnaissance-contenus.htm.

[37] DSM Directive at Article 17(5)(b).

[38] DSM Directive at Article 17(7) provides:
"The cooperation between online content-sharing service providers and right holders shall not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation.
"Member States shall ensure that users in each Member State are able to rely on any of the following existing exceptions or limitations when uploading and making available content generated by users on online content-sharing services:
"(a) quotation, criticism, review;
"(b) use for the purpose of caricature, parody or pastiche."

[39] For a user community perspective on the "dialogue" discussions, see Laureline Lemoine, *Copyright stakeholder dialogues: Compromise, frustration, dead end?*, EUROPEAN DIGITAL RIGHTS (EDRi), 26 February 2020, available at https://edri.org

[40] IViR [Institute for Information Law], University of Amsterdam, *Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics*, November 2019, available at https://www.ivir.nl/recommendationsarticle17/. The actual recommendations from the seven law professors are available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484968.

mission envisioned by Article 17. And the answer to that question depends on what these systems would look like.

In the February hearing, one witness said she was "aware of no feasible proposals for complying with the new standards that will continue to allow service providers to offer the services that Europeans and Americans have come to count on."[41] But as members of this Committee and its staff are aware that there is already one "feasible proposal" up and running: YouTube already employs a notice-and-stay down system called ContentID.

Google acquired YouTube in October 2007 and very quickly began working on means to identify unauthorized copyrighted material on the site. Early efforts using technology from Audible Magic gave way to a Google engineering project to create "video identification technology" intended to "identify copyrighted material, after which media companies can decide if they would like to remove the material or keep it up, as part of a revenue-sharing deal with YouTube, which can sell advertising alongside it."[42] In the current ContentID system, "[v]ideos uploaded to YouTube are scanned against a database of files that have been submitted to us by content owners."[43] Initially the matching system used audio only, but now also matches for video. Google claims that ContentID "can now even detect melodies, helping further stymie bad actors' efforts to fool the system."[44]

The reference files provided by copyright owners include metadata "describing the content and what action [the copyright owner] wants YouTube to apply when ContentID finds an appropriate match."[45] In most cases, the Content ID match means that the party claiming to be the copyright owner will receive a percentage of the ad revenue from streams of the uploaded audiovisual work. In the case where a party claims copyright in the music used in, say, an original home video, the uploader "may be able to share the advertising revenue with the music's copyright owners."[46] But Content ID also allows the copyright owner to decide whether it wants the audiovisual content available on YouTube.

Although these numbers have been constantly changing (upwards), as of mid-2019 YouTube claimed that Content ID had "9,000+" participating rights holders who have submitted "more than 75 million active reference files" leading to claimed ownership rights of some level over 800 million files uploaded to YouTube.[47] (In other words, at least in the case of popular works, users upload the same material over and over to YouTube.)

No one questions that ContentID is a system "in accordance with high industry standards of professional diligence" so – as an example of Article 17's application – I believe that Article 17's real impact on YouTube will be on two fronts, one beneficial to copyright owners and one potentially beneficial to YouTube users. The benefit for copyright owners is that Article 17 should push YouTube to allow *all* copyright owners to use ContentID, not just select partners. And losing its ability to withhold ContentID may mean that YouTube loses its greatest leverage over copyright

---

41 Litman Statement at 12.

42 Kenneth Li & Eric Auchard, *YouTube to Test Video ID with Time Warner, Disney*, REUTERS, June 12, 2007, available at http://www.reuters.com/article/us-google-youtube-idUSWEN871820070612; Kevin Delaney, *YouTube to Test Software To Ease Licensing Fights*, THE WALL STREET JOURNAL, June 13, 2007, available at http://www.wsj.com/articles/SB118161295626932114.

43 How Content ID works, YOUTUBE HELP, https://support.google.com/youtube/answer/2797370?hl=en

44 How Google Fights Piracy at 6.

45 How Google Fights Piracy at 26.

46 What is a Content ID claim?, YOUTUBE HELP, https://support.google.com/youtube/answer/6013276.

47 YouTube for Press, YOUTUBE, https://www.youtube.com/intl/en-GB/yt/about/press/

owners in negotiations over licensing payments. The benefit for YouTube users is that Article 17's strictures on ensuring that uploaders can enjoy copyright exceptions for "quotation, criticism, review . . . caricature, parody or pastiche" should push YouTube toward a more transparent, expeditious system to handle disputed ContentID claims.

Of course, ContentID and Audible Magic[48] not be the only acceptable systems to meet Article 17's requirements. Detractors of Article 17 pessimistically assume that filtering systems adequate to meet "high industry standards of professional diligence" will be generally unavailable and/or prohibitively expensive.[49] But Article 17 embodies a flexible standard that takes account of the platform's audience, the types of works involved, and "the availability of suitable and effective means and their cost for service providers."[50] Relatively small hosting sites are already using filtering technologies that arguably meet this flexible standard.[51] The French government has already made it clear that it intends to support the development of more filtering technologies for websites.[52] At a minimum, this is a question that should be researched and explored, not assumed. For example, it would be easy for the subcommittee to ask USPTO for an analysis of the patenting in these technologies.

One thing should not be underemphasized: a real concern with any filtering system is the problem of false positives. But this will not be a new problem with Article 17 or for any country that adopts Article 17-like measures in relation to some platforms: it is exactly the same problem as inaccurate take-down notices generated by automated infringement detection systems. In her February statement, Professor Tushnet narrated a series of false positive takedown notices[53] that reads like the mishaps, mistakes, and malfeasance in the cases that come before Judge Judy. Because any automated infringement detection system used to generate §512 notices can be used as the basis for a filtering system, that litany of false positives should tell us much about filtering systems that are not acceptable. For example, filtering based on title or key words is technologically "dumb"; using such technology should not be compatible with "high industry standards of professional diligence." In contrast, using sophisticated photograph identification software like "TinEye"[54] as the basis for a filtering system to find unauthorized postings of photos might be a boon for independent

---

[48] Still a leading player in these technologies. See https://www.audiblemagic.com/newsroom/news/.

[49] With that premise as a springboard, some scholars argue that imposing Article 17 responsibilities on YouTube, Vimeo, Instagram, and Facebook will make competitor entry even more difficult, further cementing the dominant position and profitability of these platforms. Since Facebook and Google strongly opposed Article 17 in Europe, scholars who make this argument are literally saying that they know what's best for these companies better than the companies' leadership do. I think we should be more modest and assume that people lobbying for or against something know what's in their own best interest.

[50] DSM Directive at Article 17(5)(b).

[51] *See, e.g.* Ventura Content v. Motherless, Inc., 885 F.3d 597, 616 (9th Cir. 2018) (describing a medium-sized pornography hosting site with about 611,000 visits daily visitors that, after receiving a DMCA takedown notice, disables the identified content and "uses 'hashing' software so that copies of the image or clip will be removed and will be screened out if anyone tries to post them again.")

[52] *See, e.g.* Marc Rees, *Directive Droit d'auteur : déjà une mission Hadopi-CNC-CSPLA sur la reconnaissance des contenus*, NEXTINPACT, March 28, 2019, available at https://www.nextinpact.com/news/107746-directive-droit-dauteur-deja-mission-hadopi-cnc-cspla-sur-reconnaissance-contenus.htm.

[53] Tushnet Statement at 32-39.

[54] https://tineye.com.

photographers – one of the groups of creative professionals hardest hit by internet piracy – with relatively few false positives.[55]

PARALLELS TO OTHER DMCA PROVISIONS IN OTHER COUNTRIES

While the new Digital Single Market Directive marks a disruption of the global consensus on intermediary liability and does warrant your careful study, the topic of today's hearing is more general: how other countries are handling digital piracy. In this respect, I think that the subcommittee should consider other elements of §512 that have not developed to the degree or in the way many of us expected in 1998.

One of those elements is §512(j) which balanced the §512(a)-(d) shielding of ISPs from monetary damages with making them expressly subject to different sorts of injunctive orders. In particular, §512(j)(1)(B) makes transmission ISPs eligible for injunctive orders to deny access to subscribers engaged in infringing activity "by terminating the accounts of the subscriber or account holder that are specified in the order" as well as eligible for orders "restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States." I believe that §512(j)(3) makes it clear that these orders were intended to be "innocent" third party injunctions available without suing the ISP.[56]

While there are both procedural complexities and sensitive freedom of expression concerns here, injunctions ordering ISPs to disable access to websites that predominantly promote copyright infringement have been reviewed and upheld by courts in a number of democratic societies with robust freedom of expression, including – but not limited to – the Danish Supreme Court,[57] the

---

[55] In saying this, I am assuming that the appellate court trend sharply limiting claims of "transformative use" in unaltered photographs will hold. See Monge v. Maya Magazines, Inc., 688 F.3d 1164, 1176 (9th Cir. 2012); Balsley v. LFP, Inc., 691 F.3d 747 (6th Cir. 2012); Brammer v. Violent Hues, 922 F.3d 255 (4th Cir. 2019).

[56] I assume that the lawsuit would be brought formally against the pirate website or the ISP subscribers who are engaged in infringement and the ISP would have to count as "other persons who are in active concert or participation with" the defendant under Rule 63(d) of the Federal Rules of Civil Procedure. But I am not an expert in civil procedure.

[57] U.2010.2221H, Judgment of the Danish Supreme Court, 27 May 2010 (confirming an injunctive order against the service provider Telenor requiring Telenor to disable access to www.thepiratebay.org). See also U.2006.1474H, Judgment of the Danish Supreme Court, 10 February 2006 (confirming that the service provider TDC's exemption from liability under Danish implementation of the E-Commerce Directive did not exempt TDC from an injunction to disable access to websites with illegal information); U.2015.1045.S, Judgment of the Danish Maritime and Commercial Court (Case A-38-14), 11 December 2014 (ISP Telia Denmark ordered to block access to UK-based online store based on copyright infringement).

Helsinki Court of Appeals,[58] the Paris Regional Court,[59] the New Delhi and Madras High Courts,[60] and the High Court of Justice of England and Wales.[61] Given the widespread use of this enforcement tool in other democratic societies, it may be worthwhile for the subcommittee to explore why §512(j) has not been utilized.

In February, you also received considerable testimony about federal courts' interpretation of "red flag" awareness under the DMCA. I agree with Judge Damich that the idea of "awareness" of infringement in 1998 implicitly involved visual inspection;[62] I also agree that awareness of infringement will be contextual.[63] But "context" will not always make infringement harder to see; sometimes context makes infringement more obvious (as when a tentpole studio film just released in cinemas appears online). The subcommittee might profitably look at how courts in other countries have approached this problem – my impression is that courts from France to China have had a more common sense approach to when a platform should be aware it is hosting or transmitting unauthorized materials.[64]

---

[58] Decision of the Helsinki District Court 11/41552 of October 26, 2011. On the basis of Section 60(c) of the Finnish Copyright Act, the court ordered one of Finland's biggest telecommunication providers, Elisa, to prevent access to Pirate Bay webpages. The decision was affirmed by the Helsinki Court of Appeals, decision number 1687, S 11/3097, June 15, 2012 and the Finnish Supreme Court denied leave to further appeal. Subsequent decisions in Finland ordering other ISPs to block Pirate Bay websites include Helsinki District Court decisions H11/48307 and H11/51544, both on June 11, 2012.

[59] Paris Regional Court, 3rd Division, 1st Section, 2 April 2015, No. 14/08177 (interlocutory judgment ordering T411 website to be blocked by several ISPs on the grounds that T411 was virtually entirely dedicated to making available audio recordings without authorization); Paris Regional Court, 3rd Division, urgent applications section, 4 December 2014, No. 14/03236 (ordering ISPs to block access in France to websites of the Pirate Bay network).

[60] *Delhi HC restrains 30 torrent sites from hosting copyrighted content, orders ISPs to block them*, FINANCIAL EXPRESS, April 11, 2019, available at https://www.financialexpress.com/india-news/delhi-hc-restrains-30-torrent-sites-from-hosting-copyrighted-content-orders-isps-to-block-them/1545480/ ; Bill Toulas, *ISPs in India Ordered to Block Pirate Bay, Torrentz2, YTS, and 1337x*, TECHNADU, April 12, 2019, available at https://www.technadu.com/isps-india-ordered-block-pirate-bay-torrentz2-yts-1337x/64592/. In fact, Indian courts have been ordering ISPs to block pirate websites to protect new releases of Indian films for many years. Javed Anwer, *830 more websites blocked in India, many torrent links in list*, INDIA TODAY, August 25, 2016 ("Blocking of hundreds of URLs at the behest of film producers is not new in India. It has become almost routine to for film producers to approach court before release of a film and take John Doe orders, leading to the blocking of the websites. Not only torrent sites have been blocked under such orders but also image hosts, file hosts and websites that share URLs"), available at https://www.indiatoday.in/technology/news/story/830-more-websites-blocked-in-india-many-torrent-links-in-list-337177-2016-08-25; Anupam Saxena, *ISP Wise List Of Blocked Sites #IndiaBlocks,* MEDIANAMA, May 17, 2012, available at https://www.medianama.com/2012/05/223-isp-wise-list-of-blocked-sites-indiablocks/

[61] Paris Regional Court, 3rd Division, 1st Section, 2 April 2015, No. 14/08177 (interlocutory judgment ordering T411 website to be blocked by several ISPs on the grounds that T411 was virtually entirely dedicated to making available audio recordings without authorization); Paris Regional Court, 3rd Division, urgent applications section, 4 December 2014, No. 14/03236 (ordering ISPs to block access in France to websites of the Pirate Bay network).

[62] *The Digital Millennium Copyright Act at 22: What is it, why was it enacted, and where are we now,* Hearing before the Senate Judiciary Committee Subcommittee on Intellectual Property, 116th Cong. (February 11, 2020) (Statement of Senior Judge Edward J. Damich at 3).

[63] Tushnet Statement at 7-8.

[64] For example, in Christian C, Nord-Ouest Production v. SA DailyMotion, Tribunal de Grand Instance de Paris, 3eme chambre, 2eme section, July 13 2007, the court found that because "the success [of DailyMotion] necessarily involved the dissemination of works known to the public . . . DailyMotion must be considered to have the least knowledge of facts and circumstances suggesting that illegal videos are being put online." (author's translation), available at http://www.juriscom.net/documents/tgiparis20070713.pdf. In a similar fact pattern before a Shanghai court, the court reasoned that "[i]t is well known that copyright owners normally will not provide their

This also raises an interesting point that was not mentioned in any of the February statements: in 1998 it was assumed that §512(a) transmission ISPs would not have any basis to have "awareness" of copyright infringement, but we now know that transmission ISPs often know in real time a great deal about what is happening on their networks. To the degree that the subcommittee wants to reassess the knowledge and awareness components of §512 – and whether the courts have cared out Congress' intent – I would recommend some careful thinking about what transmission ISPs regularly know vis-à-vis activity on their networks. It is also time to discuss what "awareness" will mean as more and more artificial intelligence permeates platform and network operations.

THE IMPORTANCE OF SECTION 1201

Lastly, I would like to address the other branch of the DMCA, § 1201. In her written statement, Professor Jessica Litman said that the circumvention prohibition in § 1201 "has not lived up to its promise" and that "appear[s] to be doing little actual work to diminish the unauthorized copying and use of copyrighted works." I used to share Professor Litman's view – and, if you view things that way, you might conclude that copyright owners got a very raw deal in the DMCA, trading away potential ISP liability for protection of digital locks that "doesn't seem to have been an effective weapon in the fight against piracy."[65]

As you know, § 1201 prohibits the act of circumventing a "technological measure" that controls *access* to a work and separately prohibits the trafficking in products, devices, or services intended to circumvent technological measures that either control access to a copyrighted work or exercise of a § 106 copyright right. Such technological measures – or "digital locks" – were already familiar in 1998 in the form of password-protected sites like Westlaw and LEXIS/NEXIS as well as scrambled satellite transmissions, but since then a vast menagerie of technological measures (or technological protection measures – "TPMs") has emerged to protect digitized content in different ways.

In the early days, there were some serious challenges to § 1201 and similar laws in other countries. The early scholarly commentary on § 1201 predicted that the DMCA anti-circumvention provisions were going to "chill" innovation and competition badly;[66] two decades later we have smartphones, tablets, wifi, Facebook, the blogosphere, Google, drones, Instagram, ubiquitous GPS, fledgling driverless cars, and AI. In § 1201's early days, some very smart legal minds made some spectacularly wrong guesses about how the provision would work.[67]

---

cinematographic works to the public for free viewing; the defendant both reviews and recommends uploaded videos, so it has power to control the infringement; the defendant established a channel of 'original videos' and the channel for 'movies', so it should have known that movies would be uploaded without license.." Xinchuan On-line Co. v. Tudou.com, Shanghai No.1 Intermediate Court (2008) (author's translation).

[65] Litman Statement at 5.

[66] *See, e.g.* 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."); 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 . . . .").

[67] William Landes and Judge Richard Posner guessed that digital locks would not be used on copyrighted works until the work was ready to fall out of copyright. WILLIAM LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 45 (2003).

But we will never be sure exactly *how much* work § 1201 is doing in the digital economy, precisely because we do not have a "control" of a sophisticated, large digitally networked economy without § 1201-like protections. In the absence of more rigorous means to analyze § 1201's impact, I would propose that § 1201 now undergirds much of the internet economy. It supports, if not provides the bedrock for, many legitimate internet businesses today.

Audio and audiovisual streaming services – delivered via the Internet or cable television systems – are typically *encrypted* subscription-based services, meaning that "access" to the streamed content is protected by § 1201(a) technological measures. But after a transmission to the player device is decrypted, all or almost all of these streaming services employ some further technological measures to limit user's ability to convert the audiovisual stream into a download. This TPM prevents the exercise of copyright's § 106 right of reproduction. 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.[68] Such TPM preventing a *stream* from becoming a *download* is fundamental to streaming business models – Netflix, Hulu, Disney+, CBS All Access, Spotify, Amazon Prime, etc.

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 a television or monitor, 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 device will almost be 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, a device or 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 (called a "link" DRM). If the television or monitor 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.[69]

And effective digital locks are not just important to commercial enterprises. Today, 43,000 libraries and educational institutions provide e-book lending services through Overdrive: digital copies of books are "lent" to the library patron using § 1201(a) technological measures to limit access to a specified period of "lending,"[70] not too different from the way Spotify's "tethered" copies of music tracks on a consumer's device will self-delete if the Spotify account is not maintained. Technological measures are also used by the blind community and its service providers to ensure

---

[68] For Apple's "Fairplay" streaming TPM, see https://developer.apple.com/streaming/fps/. For Microsoft's "Playready" TPM, see https://www.microsoft.com/playready/. For Google "Widevine" TPM, see https://www.widevine.com. To be clear, the TPM used will be specific to the app, so one might have an app using Playready although the app is running on an Android device.

[69] For a fuller discussion of TPM usage, see Justin Hughes, *Motion Pictures, Markets, and Copylocks*, 23 GEORGE MASON L. REV. 941, 950-966 (2016).

[70] https://company.overdrive.com/company-profile/who-we-are/. With these TPM-protected ebooks, "[t]itles you've borrowed from the library will automatically be returned at the end of their lending periods," *How to Return a Downloaded Title Using OverDrive for Android*, OVERDRIVE, available at http://help.overdrive.com/customer/en/portal/articles/1482571- how-to-return-a-downloaded-title-using-overdrive-for-android.

that "accessible format" copies under 17 U.S.C. §§ 121 and 121A are "used exclusively" by persons who are blind or are otherwise eligible under those provisions.

For all these reasons, I agree with Jonathan Band that "TPMs have been extremely helpful to the development of legitimate digital business models";[71] where I respectfully disagree with Jonathan is his conclusion that "the critical element has been the technological protection provided by TPMs, not the legal prohibition on circumvention and circumvention tools."[72] Instead, I think that we can guess what would have happened without § 1201 in light of our experience in the past 20 years – an experience of technologists again and again testing legal limits, from the Aereo platform[73] to electric scooters.[74] My guess is that §1201 is what has prevented digital lock picks from being built into browsers and available on apps stores; my guess is that § 1201 has saved us from an ugly, wasteful tech race of digital locks and lock picks. Professor Litman reported to you that "[p]rohibited circumvention tools are widely available, and widely regarded as legitimate."[75] She may be right; it depends on what she meant by "widely" and I do not know what empirical evidence she has (both on dissemination of lock picks and on public attitudes). But we should consider the possibility that § 1201 works like the *Grokster* decision:[76] it depresses commercial business models built on the prohibited activity, while less than 100% enforcement means the prohibited activity will continue at some level.

REFINING SECTION 1201 AND WHAT OTHER JURISDICTIONS ARE DOING

While I believe that § 1201 is an important legal structure for the digital networked economy, I agree with some of your February panelists that Congress could meaningfully improve the contours of § 1201 coverage and tweak – or even rethink – the triennial process by which the Librarian of Congress, in conjunction with the Department of Commerce, grants exceptions from § 1201(a) liability.

First, I share the concern of some of your February panelists on the problem of "embedded" software[77] and I think that the subcommittee could profitably study the question of how to amend

---

[71] *The Digital Millennium Copyright Act at 22: What is it, why was it enacted, and where are we now,* Hearing before the Senate Judiciary Committee Subcommittee on Intellectual Property, 116th Cong. (February 11, 2020) (Statement of Jonathan Band at 7, fn. 8).

[72] *Id.*

[73] American Broadcasting Companies v. Aereo, 573 U.S. 431 (2014).

[74] Petula Dvorak, *The electric scooters swarming our city won't solve our commuting calamity*, WASH. POST, August 27, 2018 ("The main scooter companies — born in the West Coast's tech sector — soft open their product by dropping the scooters in cities, then negotiat[e] with frazzled city councils later."), available at https://www.washingtonpost.com/local/the-electric-scooters-swarming-our-city-wont-solve-our-commuting-calamity/2018/08/27/fb7fbf32-aa12-11e8-a8d7-0f63ab8b1370_story.html; Peter Holley, Hospital ER reports 161 percent spike in visits involving electric scooters, WASH. POST, September 24, 2018 ("Emergency physicians in a dozen cities around the country have told The Washington Post that they are seeing a spike in scooter accidents."), available at https://www.washingtonpost.com/technology/2018/09/24/hospital-er-reports-percent-spike-visits-involving-e-scooters/.

[75] Litman Statement at 5.

[76] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[77] Tushnet Statement at 25-26; Litman Statement at 7.

§ 1201 to address this issue.[78] Simply put, § 1201 was not drafted in 1998 with a complete appreciation of the degree to which software would be embedded into everyday appliances and medical devices as well as farming and business equipment. Congress has solved a parallel kind of puzzle before – in the software rental exception to the first sale doctrine codified in § 109[79] – and I believe that you can do it again.

Second, the § 1201(a)(1)(C) triennial process for granting exemptions from § 1201(a)(1)(A) liability could be improved. For example, instead of a *de novo* triennial application process, there could be a more institutionalized presumption that 3-year exemptions are renewed absent meaningful proof that there has been a change in the relevant factors in § 1201(a)(1)(C)(i - v). Congress could also amend § 1201(a)(1)(D) to clarify how the exemptions should be defined in relation to specific kinds of users, uses, and works. More broadly, this subcommittee might consider whether a different system for granting exemptions would be less strain on the Copyright Office while better serving both copyright owners and users of copyrighted works. A number of sophisticated copyright laws protecting TPMs provide the "safety valve" of § 1201(a)(1)(C) through administrative processes that can be utilized at any time – and, therefore, do not produce regular crescendos of work for the administrative agency granting exemptions. For example, Singapore and Norway each have an on-going administrative process which can receive applications for circumvention exemptions at any time.[80]

---

[78] But I have no opinion on whether or not there should be a general or default "right to repair"; I think it is reasonable for a consumer to purchase a product with the condition that she will only have repairs done by an authorized entity – as long as she knows about and consents to that condition.

[79] 17 U.S.C. § 109(a) codifies the "first sale" doctrine that "the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord." In the case of sound recordings and computer programs, § 109(b)(1)(A) then excludes from this freedom any "dispos[ing]" of the copy "by rental, lease, or lending, or by any other act or practice in the nature of rental, lease, or lending." Section 109(b)(1)(B) then excludes from the exclusion "a computer program which is embodied in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product" as well as "a computer program embodied in or used in conjunction with a limited purpose computer that is designed for playing video games and may be designed for other purposes."

[80] Section 100 of the Norwegian Copyright Law of 2018 provides "Right holders shall ensure that beneficiaries who have legal access to a protected work, without hinder by an effective technological protection measure, can use the work, hereunder produce new copies, pursuant to §§ 32 to 34, 40, 43, 45, 48, 49, 55, 56, and 5If the right holder after a petition from a beneficiary of a section listed above fails to provide access as described in the first paragraph, he can, on the beneficiary's petition, be ordered to provide such information that is necessary to enable the work to be used in accordance with the objective. The petition shall be addressed to the Board established by the Ministry pursuant to regulations the King may issue. The Board can in addition to orders as mentioned, rule that the beneficiary without hinder under section 99 can circumvent the applied technological protection measures if the right holder fails to adhere to the time limit imposed by the Board to comply with the order." LOV-2018-06-15-40: Lov om opphavsrett til åndsverk m.v., (author's translation), available at https://wipolex.wipo.int/en/text/504083. Similarly, section 261D(2) of the Singapore Copyright Act provides that "The Minister may, by order published in the Gazette, exclude the operation of section 261C(1)(a) in relation to a specified work or other subject-matter or performance, or a specified class of works or other subject-matters or performances, if he is satisfied that any dealing with the work, subject-matter or performance or with the class of works, subject-matters or performances, being a dealing which does not amount to an infringement of copyright therein or an unauthorised use thereof (as the case may be), has been or is likely to be adversely impaired or affected as a result of the operation of this section." Singapore Copyright Act (Chapter 63), available at https://sso.agc.gov.sg/Act/CA1987?ProvIds=P1XIIIA-#pr261D-.

CONCLUSION

In my view, application of the DMCA to the digital, networked environment has held up surprisingly well despite extraordinary technological developments, completely unpredicted business models, and some occasional strange court decisions. But the old paradigms of internet service providers, especially the paradigm of web "hosts," do not fit particularly well with the media and social network giants that have emerged since 1998. In addition to considering whether it is time for the United States to rethink its categories of internet service providers as the European Union has, now is a good time to start exploring how § 1201 might be made more user-friendly without jeopardizing the substantial role it plays in defining digital markets, how knowledge and awareness might be reconceptualized for increasingly "intelligent" platforms, and how we can profit from copyright enforcement practices in other countries.

# # # #