Letter from the Editor

By Brian Rosenblatt

This issue brings to a close Volume 33 of The Entertainment and Sports Lawyer. The past year has been one filled with changes, predictions, and confirmation.

In October, the Forum held its Annual Meeting, “The Year of Thinking Big” in Washington, D.C., and it did not disappoint. I am pleased, with this issue, present a series of Law Students’ Perspectives on various panels, synopses of the Conference, and even fresh ideas on pending “hot topics”.

Our lead article, “Program Access and Program Carriage”, by Jennifer Scullion, is Part I of a two part series that takes a look at how the Program Access regime has been nimbly retooled in multiple rounds to strike the right balance between protecting against potential vertical-integration abuses and yet allowing industry participants to address legitimate business concerns and respond creatively to a rapidly changing market. The result is a marketplace more than two decades later that is more competitive than ever before—and preparing for still more to come as internet linear and on-demand video services continue to grow.

We follow that with a fascinating read from Professor John T. Wendt, with editing assistance from law student Lionel Yarmon. Professor Wendt looks at the various failures of the Sochi Olympics as a framework the pending for the 2016 Olympics. The road to Sochi revealed many issues that must be addressed for future Olympics including the cost of preparing for the Games, political disputes having the effect of separating rather than unifying participating nations, selection of the Olympic events, ongoing drug concerns, and the safety of the athletes and spectators. In only eight months, the 2016 Summer Olympics will be held in Rio de Janeiro, Brazil. Rio finds itself facing many of the same concerns that surfaced in Sochi with the three most prominent being Rio’s venue and infrastructure viability, the continued war on doping, and the call for greater transparency and reform in sports’ governing bodies. With this in mind, it is worth reflecting on the Games in Sochi to better understand the challenges the Olympic Games and its host nations continue to face. This article will be followed in the next issue with a more specific look into the Rio Games.

We are also pleased to present a two-pronged look at the lasting impacts of the Sony Hack. Maia Spilman and Zelda Gerard have captured both national and international perspectives in parallel for what has been an all-consuming data breach.

For our Law Students’ Perspectives Series, Law Student Preston Barclay provides us with a review and predictions for daily betting fantasy sports; Daphne Bugelli discusses Performance Rights; Lauren Nevidomsky reviews the ins and outs of being team counsel for professional sports organizations; and Hollyn Randolph provides her perspectives on the Forum’s 2016 Annual Meeting.

Finally, we close the issue with Michelle Wahl’s perspective on recent litigation, particularly a summary of a handful of recent case rulings which are impacting the legal landscape for the entertainment and sports industries.

I would like to remind all Forum Members and readers that we are always searching for authors and articles.

Brian A. Rosenblatt
Deutsch, Levy & Engel, Chtd.
BrianRosenblatt@dlc.com
Editor-in-Chief, Entertainment and Sports Lawyer

Brian Rosenblatt is a Chicago attorney with the firm of Deutsch, Levy & Engel, Chtd. Brian serves as the Editor-in-Chief of the Entertainment and Sports Lawyer.
Program Access and Program Carriage Nearly 25 Years In, Where Do the Fraternal Twins of Video Programming Distribution Stand?

By Jennifer Scullion

Part One

In the early 1990s, there was concern that two aspects of the cable industry might hamper the development of new, competing "multichannel video programming distribution" ("MVPD") technologies, such as direct broadcast satellite ("DBS") services (e.g., DirecTV and DISH) or "wireline" services (e.g., Verizon FiOS and AT&T U-verse). First, cable was the dominant means for such distribution nationally, as well as in most local market (due to local franchising requirements). Second, there was a substantial amount of vertical integration of cable operators and programming vendors. This provided the potential for incumbent, inter-related players to deny new distributors "access" to desirable programming and, thereby, hamstring their ability to compete for subscribers. Finally, as the MVPD industry continued to grow, operators might try to increase their actual or effective control over programmers, squeezing out independent programming and, thereby, diminishing programming competition and diversity.

To address these concerns, the Cable Television Consumer Protection and Competition Act of 1992 (the "1992 Cable Act") put in place two related, but distinct, regimes: "Program Access" and "Program Carriage." Broadly speaking, "Program Access" protects MVPDs by ensuring a certain degree of "access" to programming. Thus, the complaining party in a Program Access proceeding is the MVPD. By contrast, Program Carriage polices MVPDs with respect to their treatment of programming vendors in contracting for carriage of programming. In a Program Carriage proceeding, the MVPD is the respondent.

For nearly twenty-five years, the Program Access and Program Carriage rules have evolved through four administrations, eight FCC Chairs, the tremendous expansion of video distribution and programming choices, and ever-changing technologies. And they have done so in decidedly very different ways.

The Program Access regime has been nimbly retooled in multiple rounds to strike the right balance between protecting against potential vertical-integration abuses and yet allowing industry participants to address legitimate business concerns and respond creatively to a rapidly changing market. The FCC's Program Access rules and actions have overwhelmingly survived challenges based on the First Amendment and Administrative Procedure Act. And, for the most part, Program Access proceedings have been brief and resolved without hearing or multiple appeals. The result is a marketplace more than two decades later that is more competitive than ever before—and preparing for still more to come as internet linear and on-demand video services continue to grow.

By contrast, the Program Carriage regime has ground along at a slow, deliberate pace, focusing on factually intense issues of whether video programmers have been "coerced," "retaliate[ed] against," or the targets of discrimination "on the basis of affiliation" that "unreasonably restrains" the programmer’s ability to "compete fairly." Exceedingly few proceedings have been brought and not a single, reported victory for the protected class (unaffiliated programmers) has ever survived the multi-layer appeal process. Yet, it would be hard to argue that the video programming industry lacks fresh, high quality, and extremely diverse sources of content. The critical question now is whether the Program Carriage regime (or some form of it) can and should be used to ensure continued program diversity and competitiveness as the distribution arm of the industry skinnies up, repackages, and revamps to compete with the growing field of new services.

This article proceeds in two parts. Part One reviews the Program Access regime and its current status and key issues. Part Two (in a forthcoming issue) will turn to the Program Carriage regime and compare the progress and issues there.

I. The Program Access Regime

A. Preliminaries

Before delving into the structure and substance of Program Access, two preliminary points for orientation are helpful.

First, some useful navigation. The “Program Access” regime is rooted in Section 628 of the Communications Act of 1934, 47 U.S.C. § 548. It is implemented by the FCC under its “Program Access Rules,” 47 C.F.R. § 76.1000-1004, which set forth applicable definitions, the substantive standards, and rules governing FCC adjudication of Program Access complaints.

Second, some (hopefully) useful terminology and distinctions to parse the exceedingly dense language of the Program Access statute and rules.

MVPDs: The Program Access regime protects MVPDs. As discussed below, the FCC currently is considering whether and to what extent so-called “Over The Top,” internet-based distributors fall within the definition of MVPD. More
generally, however, the FCC’s rules provide that certain representatives of MVPDs—“buying groups” and “agents”—are deemed MVPDs for Program Access purposes. 47 C.F.R. § 76.1000(c), (e).

Cable Operators: The Program Access regime principally targets cable operators and their affiliated programming vendors. However, Congress also extended the Program Access provisions to “common carriers” (e.g., AT&T, Verizon, etc.) and their “affiliates” if the common carrier (or affiliate) “provides video programming by any means directly to subscribers.” 47 U.S.C. § 548(j); 47 C.F.R. § 76.1004.” To date, common carrier MVPDs have not had significant market power, nor have they been vertically integrated with programming vendors. Therefore, the Program Access rules have remained focused on cable operators and their affiliated programming vendors. The recent acquisition of DirecTV (which has interests in multiple networks) by AT&T will bring all of the former DirecTV networks under the Program Access regime.iii

“Satellite” v. “Terrestrial” Programming: Section 548 repeatedly refers to “satellite” cable programming. These are not references to programming delivered by satellite to subscribers (e.g., DBS services such as DirecTV or DISH). Rather, the “satellites” at issue are those that deliver programming to cable systems, which in turn distribute the programming by various means to subscribers. The vast bulk of the programming consumers watch through their cable or other MVPD service is, thus, “satellite” programming. However, some programming, particularly local or regional programming such as “regional sports networks,” is delivered to MVPDs terrestrially. As discussed below, concerns were expressed for many years about the extent to which the Program Access regime could or would apply to programming delivered through the so-called “terrestrial loophole.” Following a series of FCC Orders in 2010 and 2012, the core Program Access provisions now apply equally to all programming regardless of how it is delivered to the MVPD system.

B. The Structure of the Program Access Regime

The purpose of the Program Access regime is to “increase[e] competition and diversity” in the market for “multichannel video programming” and to “spur the development” of video distribution technologies. 47 U.S.C. § 548(a). Congress also sought to “increase the availability” of cable and broadcast programming to rural areas. Id.

Mindful that the video programming and distribution industries were (and are) complex, and that a central purpose of the Program Access provisions was to foster changes in the both the “upstream” and “downstream” markets, Congress sketched out the Program Access regime in broad contours, leaving it to the FCC to determine how best to address Congress’ concerns about the potential impact of vertical integration.

1. General Prohibition on Unfair Acts and Practices

The heart of the Program Access regime is Section 548(b). Section 548(b) is targeted at “cable operators” and their affiliated programming vendors. It broadly declares that “unfair methods of competition” and “unfair or deceptive acts or practices” by such operators and vendors are “unlawful” when the “purpose or effect” of such conduct is to “hinder significantly” (or actually prevent) any MVPD from providing “satellite cable programming” or “satellite broadcast programming” to subscribers or consumers. 47 U.S.C. § 548(b).

Congress did not attempt to catalogue the types of conduct that would violate Section 548(b) or even dictate standards and criteria to be used to determine whether there was a violation. Instead, it directed the FCC to promulgate regulations “to specify particular conduct that is prohibited by [Section 548(b)].” 47 U.S.C. § 548(c)(1). Congress did, however, require that such regulations include a few, key provisions. The specific prohibitions directed by Congress in Section 548(c) are discussed below.

Before turning to the specific prohibitions, it is important to observe several overarching points about Section 548(b):

- Section 548(b) applies to all “cable operators.” By contrast, the specific prohibitions of Section 548(c) apply only to vertically integrated cable operators (i.e., those with an “attributable interest” in a programming vendor).vi

- But unlike the specific prohibitions of Section 548(c) ---which are considered “implicitly harmfulvii---, an MVPD asserting a violation of Section 548(b) must prove harm. Specifically, an MVPD must prove that the challenged conduct has the actual purpose or effect of “hinder[ing] significantly” or preventing an MVPD from providing programming to consumers.

- In 2010, the FCC sought to close the so-called “terrestrial loophole” by interpreting Sections 248(b) to apply to conduct that directly affected terrestrial delivered programming---such as an exclusive license for cable-affiliated, terrestrial sports programming---on the theory that such conduct might nonetheless significantly “hinder” an MVPD in their general business of providing satellite delivered programming to subscribers.viii
In 2011, the D.C. Circuit largely upheld the FCC’s interpretation of Section 548(b) as reasonable. As such, conduct implicating terrestrially delivered programming is no longer exempt from the Program Access regime and may be challenged under Section 548(b).

However, the D.C. Circuit rejected the FCC’s additional attempt to apply Section 548(c)’s specific prohibitions to terrestrially delivered programming (by deeming such conduct categorically “unfair” for purposes of Section 548(b)).

Although the FCC has generally embraced a case-by-case approach to Section 548(b) complaints, there is a growing trend toward creating more formal rules and presumptions to govern the agency’s analysis.

In 2010, the FCC (1) established a rebuttable presumption that withholding a terrestrially delivered regional sports network (“RSN”) affiliated with a cable operator had the “purpose or effect” of “significantly hindering or preventing” the MVPD from providing programming to subscribers and (2) ruled that conduct affecting SD and HD versions of the RSN could be evaluated separately for the purpose of a Section 548(b) complaint.

In 2012, the FCC expanded the RSN rebuttable presumption to satellite delivered RSNs affiliated with cable operators and, more generally, ruled that SD and HD versions of networks would be examined separately in assessing whether an exclusive contract between a cable operator and a cable-affiliated programmer violated Section 548(b).

In 2012, the FCC also proposed to adopt a series of additional rebuttable presumptions with respect to regional and national

2. Specific Prohibitions (Section 548(c)(2))

a. Undue Influence (Section 548(c)(2)(A))

To avoid the potential abuse of vertical integration within the cable industry, Congress sought to prevent a cable operator from exerting undue influence on an affiliated programmer. Again, however, Congress largely left it to the FCC to determine the method and degree of separation. Section 548(c)(2)(A) simply directs the FCC to “establish effective safeguards” that would prevent a cable operator from “unduly or improperly influencing” any affiliated programming vendor in deciding whether to license programming to an “unaffiliated MVPD,” or the prices, terms, or conditions of the license. The FCC has thus far given the “undue influence” provisions of Section 548(c)(2)(A) only a supporting role to potentially bolster claims of alleged violations of other aspects of the Program Access regime, such as unlawful price or non-price discrimination under Section 548(c)(2)(B).

b. Discrimination (Section 548(c)(2)(B))

Section 548(c)(2)(B) prohibits vertically integrated cable programmers from “discriminating” among MVPDs in licensing programming. However, in negotiating and setting the pricing, terms, and conditions of their agreements with MVPDs, such programmers can reasonably seek to address and account for issues such as “creditworthiness,” financial stability, technical qualifications, “actual and reasonable” cost differences, as well as “economies of scale” and other “direct and legitimate economic benefits” related to an MVPD’s subscribership. 47 U.S.C. § 548(c)(2)(B)(i)-(iii).

In contrast to the anti-discrimination provisions of the Program Carriage regime (to be discussed in Part Two), the Program Access rules do not require proof that the programmer discriminated in its dealings with MVPDs based on any affiliation or lack of affiliation of the MVPD. Instead, the FCC will find discrimination under Section 548(c)(2)(B) when:

(1) “the same or essentially the same programming service;”
(2) is sold or offered to “competing” distributors (i.e., MVPDs with overlapping local or national service areas);
(3) at different prices or pursuant to different terms or conditions;”
(4) even though the distributors are “similarly situated” such that “the differential is not justified” under one or more of the legitimate licensing considerations set forth in Section 548(c)(2)(B)(i)-(iii).

The first three elements above establish only the existence of “differential” treatment. The FCC has emphasized that “differential” treatment by a cable-affiliated programmer is not necessarily unlawful “discrimination” for Program Access purposes. To distinguish between “legitimate” differential treatment and unlawful “discrimination,” the FCC focuses on whether the competing MVPDs are “similarly situated.” Id. Factors taken into account in comparing MVPDs include, for example, what “secondary services” the MVPD is willing and able to provide as consideration for the license
When Congress enacted the Program Access regime in 1992, it was particularly concerned about the potential for the development and expansion of non-cable MVPDs to be unduly hampered by a “trifecta” of (1) national and local cable dominance, (2) significant vertical integration of cable operators and important programmers, and (3) exclusive licenses between cable operators and their affiliated programmers making it impossible for non-cable MVPDs to secure competitively important programming. To address this, the 1992 Cable Act specifically prohibited exclusive programming licenses between vertically integrated programmers and cable operators in areas served by cable operators as of October 1992, unless the programmer/operator could show that the exclusive license was in the “public interest” under a defined set of factors. Section 548(c)(2)(D), (c)(4). However, the “exclusive contract” prohibition was intended to “sunset” when (1) impasse in otherwise good faith negotiations, (2) a history of default by the MVPD with other programmers (or an extant contract dispute with the particular cable-affiliated programmer), and (3) the programmer’s “preference” simply not to sell certain programming in a particular region for reasons separate and apart from the identity of the particular MVPD seeking the license. Id. at ¶ 116.

c. Exclusive Licenses (Section 548(c)(2)(D))

When Congress allowed the Program Access regime to sunset on October 5, 2012. in re Revision of the Commission’s Program Access Rules, 27 FCC Rcd. 12605, 2012 WL 4802073 (FCC Oct. 5, 2012). In doing so, the FCC stated that the potential for anticompetitive conduct by vertically integrated cable programmers “remain[ed] a concern” for the agency. However, the FCC also observed that the market for multichannel video programming and distribution had changed substantially since 1992. Cable was far less dominant nationally, although some operators still served substantial portions of households in some local markets. And programmers affiliated with cable operators controlled a smaller portion of the overall programming universe (which exploded between 1992 and 2012), as well as a smaller portion of the most important cable and broadcasting networks. The FCC called it a “mixed picture.” Id.

As discussed below, the sunset of the Section 548(c) “exclusive contract” prohibition does not take exclusive contracts between cable operators and their affiliated programmers outside the Program Access regime entirely. When the FCC allowed Section 548(c)(2)(D) to sunset, it specifically observed that exclusive contracts remained subject to challenge under other Program Access provisions, principally Section 548(b)’s general prohibition on “unfair” competition, practices, or acts. In addition, Comcast-NBCU is effectively prohibited from exclusively licensing its networks until after 2018 because the FCC Order approving that merger in 2011 provides that any MVPD that cannot reach a programming deal with Comcast-NBCU can force the issue to arbitration in which the arbitrator’s only option is to award a carriage contract either on terms put forth by the MVPD or on terms put forth by Comcast-NBCU in baseball-style, final offer arbitration.

d. Delivery to Historically Unserved Areas (Section 548(c)(2)(C))

As noted above, one of Congress’s goals in passing the 1992 Cable Act was to encourage the delivery of multichannel video programming to areas that, at the time, were not served by cable operators. 47 U.S.C. § 548(a). These were principally rural areas that, it was hoped, would be served by the expansion of DBS or other distribution technologies (including new cable systems). To facilitate service to such “unserved” areas, the Program Access regime categorically prohibits all “practices, understandings, arrangements, and activities” by cable operators (or common carriers) that prevent any MVPD from obtaining programming from a vertically integrated programmer or broadcaster to the extent that the MVPD is seeking to deliver the programming to areas that were not served by a cable operator as of October 5, 1992. 47 U.S.C. § 548(c)(2)(C); 42 C.F.R. § 76.1002(c)(1).
The Section 548(c)(2)(C) per se prohibition applies only to satellite-delivered programming. And, again, the restrictions apply only to programmers or broadcasters that are vertically integrated with a cable operator (or common carrier).

The practices prohibited by Section 548(c)(2)(C) include exclusive licenses with cable operators, but, again, only to the extent that the exclusive license prevents another MVPD from licensing the programming for delivery to an historically unserved area. Id. Importantly, unlike the general prohibition on exclusive licenses provided under Section 548(d), Section 548(c)(2)(C)’s per se prohibition (i) has no “sunset” provision and continues, to this day, to apply with respect to areas that were unserved as of 1992 and (ii) has no “public interest” exception.

Likely because it is a per se prohibition and of limited application, the “unserved areas” provision of the Program Access regime has generated the least amount of litigation before the FCC. Only one reported decision addresses any alleged violation of Section 548(c)(2)(C). That decision, In re World Satellite Network, Inc. v. Tele-Communications, Inc., et al., 14 FCC Rcd. 13242, 1999 WL 599217 (F.C.C. Aug., 11, 1999), dismissed the complaint because the Cable Services Bureau found that World Satellite Network was not an MVPD and, therefore, lacked standing to bring a Program Access claim. Id. at 13253.

C. Program Access Proceedings

The 1992 Cable Act gives MVPDs aggrieved by an alleged violation of the Program Access provisions the right to commence an “adjudicatory proceeding” before the FCC. 47 U.S.C. § 548(d). Only MVPDs may bring a Program Access proceeding.

The FCC is required to provide “expedited review” of Program Access complaints. 47 U.S.C. § 548(f)(1). While some of the more complex proceedings have been lengthy, most Program Access complaints have been resolved in relatively short order (months) based on written submissions and discovery. Current FCC rules provide a relatively short “pleading cycle,” followed by the opportunity for discovery, and written submissions. In complaints alleging denial of programming, the FCC requires the Media Bureau to issue its decision (reviewable by the full Commission) within six months of filing of the complaint. 47 C.F.R. § 76.1003(m).

If the Program Access complaint concerns renewal of an existing carriage agreement, the MVPD may seek a “temporary standstill” when it files its complaint. The request for a temporary standstill must be made before the contract expires. As a practical matter, it is incumbent on the MVPD to make the request far enough in advance of the end of the contract to allow the programmer to respond and the Commission (or, more likely, Media Bureau) to rule. The standards for a temporary standstill are essentially identical to those for a TRO. 47 C.F.R. § 76.1003(i).

Although it has not been without its critics, the relatively expeditious Program Access proceedings stand in stark contrast to Program Carriage proceedings, which often mirror full-scale antitrust proceedings or complex commercial arbitrations in length, discovery, the use of live testimony, intensity of staffing, etc. The nature, cost, and length of the different proceedings may also account, in part, for the fact that dozens of Program Access complaints have been filed since 1992, while there have been only fifteen or so Program Carriage proceedings in the same period. The Commission is empowered to award an “appropriate remedy,” including an award establishing the “prices, terms, and conditions of sale” of programming to the aggrieved MVPD. 47 U.S.C. § 548(e)(1).

D. Key Program Access Issues

1. Definition of MVPD

One of the most (if not the most) significant changes in the video programming industry is the rapid development and deployment of new distribution technologies, platforms, and business models. If DBS and wireline distribution were the first and second waves that gradually eroded the market share of cable providers since 1992, internet-based distribution is a potential tsunami. Moreover, at least one FCC Commissioner has observed that the Program Access regime played a material role in the rise of non-cable distribution through the 1990’s and early 2000’s. Statement of Commissioner Copps re: In re Implementation of the Cable Television Consumer Protection and Competition Act of 1992, 2007 WL 2668539, at *3 (Sept. 11, 2007) (“[i]t is no exaggeration to say that without these rules, the DBS industry as we know it would not exist.”). The most significant question for the Program Access regime now is whether its protections will extend to the incoming wave of internet-based distribution.

The FCC first grappled with this issue in a 2010 Program Access complaint filed by Sky Angel. In response to a temporary standstill petition from Sky Angel, the Media Bureau found that Sky Angel could not show a likelihood of success on its complaint because only MVPDs can obtain Program Access relief and Sky Angel did not meet the definition of MVPD. Sky Angel U.S., LLC, Order, 25 FCC Rcd. 3879, 3882, 2010 WL 1622432 (FCC Apr. 21, 2010). The Media Bureau reasoned that the definition of MVPD required the operator to make multiple “channels” of video programming available to its subscribers and that a “channel” for purposes of the MVPD definition referred not just to streams of content, but to the provision of the actual transmission path. Id. at 3883 and n. 40. Based on the record before it, the Media Bureau found that Sky Angel merely provided multiple streams of programming, but it was “the subscriber’s Internet service provider” that provided the actual “transmission path” to bring the streams to the subscriber. Id.
Following its denial of Sky Angel’s petition, the Media Bureau solicited comments on how to interpret MVPD and “channel” for purposes of Program Access proceedings. 27 FCC Rcd. 3079, 2012 WL 1095923 (FCC May 30, 2012). More than two years later, in late 2014, the FCC issued a Notice of Proposed Rulemaking on the definition of MVPD more generally. In re Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services, Notice of Proposed Rulemaking, 29 FCC Rcd. 15995, 2014 WL 7331852 (Dec. 19, 2014). The FCC tentatively concluded that, for purposes of Program Access and other MVPD benefits and obligations, the definition of MVPD (1) includes “internet-based distributors” that make available “continuous, linear streams of video programming” on a “subscription basis” and (2) applies regardless of whether the distributor also provides the “transmission path” itself for delivery of the streaming video. Id. at ¶ 18.

As the FCC recognized, interpreting the Program Access rules to apply to internet-based, linear video subscription services raises a host of issues, including:

- Whether cable-affiliated programmers would be forced to negotiate programming licenses with large number of new, internet MVPDs;

- Whether extending Program Access to internet MVPDs would impact the value of the cable-affiliated programming (e.g., Bravo) licensed to other MVPDs, as well as the value of cable-affiliated programming in comparison to non-cable-affiliated programming (e.g., Game Show Network);

- Whether granting internet MVPDs Program Access rights would provide an unwarranted competitive advantage over incumbent MVPDs with different cost structures and commitments or, conversely, whether excluding internet MVPDs from the Program Access regime would grant traditional cable, DBS, and wireline MVPDs an undue advantage and stall innovation; and

- Can cable-affiliated programmers sufficiently protect the security of their programming for transmission over the internet without undue risk of Program Access complaints claiming violations of Sections 548(b) and (c)(2)(B)?

2. Proof of Harm

The FCC has shed surprisingly little light on the what is required to prove that “unfair” conduct under Section 548(b) has the “purpose or effect” to “hinder significantly” the ability of a complaining MVPD to provide video programming to customers. For many years, Section 548(b) largely played only a supporting role. Since 2010, however, the agency has moved Section 548(b) out front and center in the Program Access regime. And, if internet-based distributors are brought under the Program Access umbrella, the reliance on Section 548(b) is only likely to increase further.

The agency has explained only that the evidence needed to prove this element of a Section 548(b) claim “will vary based on the facts and circumstances of each case and that the appropriate facts and analysis may depend on whether the MVPD is a new entrant (more vulnerable to be “hindered,” but potentially harder to prove what would happen in the but-for world) or an “established competitor, as well as whether the specific programming at issue is new (harder to prove value and potential impact on MVPDs and potentially more likely to justify at least short-term exclusive contracts) or old. In re Review of the Commission’s Program Access Rules and Examination of Programming Tying Arrangements, 25 FCC Rcd. 746, 2010 WL 236800 (FCC Jan. 20, 2010). It also has suggested that the potential for conduct to “hinder” an MVPD may be show thru regression analyses showing how the MVPD’s market share would improve with the programming or, conversely, surveys estimating the likelihood that customers either would not subscribe to or would switch away from an MVPD that did not carry the programming at issue. In re Matter of Revision of the Commission’s Program Access Rules, 27 FCC Rcd. 12605, 12642, 2012 WL 4802073 (FCC Oct. 5, 2012).

On its face and in context, “hinder significantly” cannot require proof, for example, that an MVPD will go out of business (in the relevant locale or completely). Conduct that takes an MVPD out altogether “prevents” delivery of programming. But Section 548(b) allows an MVPD to proceed under Section 548(b) if the conduct would either “prevent” or “hinder significantly” deliver of programming, so “hinder significantly” must mean something less than drive an MVPD out of business.

On the flip side, how low is the threshold to prove significant hindrance? For a new MVPD entrant, is it enough that the conduct makes it somewhat more difficult to secure subscribers or must the complaining party in that case prove or must it show that the conduct is closer to a barrier to entry? For new entrants or established competitors, should the FCC consider how the conduct may impact the relative margins of the complaining MVPD and its competitors? What is the import of whether the programming at issue is “replicable” and what makes non-sports programing “replicable”? How is significant hindrance assessed in cases that do not involve withholding or denial of programming?
3. What Is “Unfair”? 

In the early years of Program Access, the specific prohibitions of Section 548(c) loomed larger. Now Section 548(b)’s general prohibition on “unfair” conduct takes center stage. As the industry transforms, we can expect to see greater resort to Section 548(c) proceedings. A critical question will be what are the limits of what is “unfair”? 

Some edges have been staked out. Past decisions have held that conduct “permitted” by other sections of the Communications Act or the Commission’s rules “cannot, without more, form the basis of a claim of unfair competition.”xv Nor can Section 548(b) be used to circumvent or interfere with “non-frivolous” contract disputes.xvi

The decisions also have resisted allowing Section 548(b) to expand into an FCC version of Section 5 of the FTC Act. For example, in In re Am. Cable Co., supra, the Cable Services Bureau rejected a challenge by one cable company to three-year, discounted plans offered by a competitor. The Bureau found that the complaining party had not shown a sufficient “nexus” between the challenged conduct and the ability of the complaining party to distribute satellite cable programming and that challenges to “rate” issues were governed by a separate provision of the Communications Act (Section 623(d)). But, to justify expanding Section 548(b) to eliminate the “terrestrial loophole,” the FCC seemed to lower the threshold to allow a relatively attenuated “nexus” to invoke Section 548(b). Thus, the coming years may see a series of new and creative Section 548(b) theories further and further afield from actual interference with program access.

A potential harbinger of a new, “creative” approach to Section 548(b) was seen in DISH’s 2010 program access complaint.xvii DISH claimed that MSG insisted on negotiating for carriage only of a “tied” set of channels. DISH alleged that the “tying” was an unfair practice that violated Section 548(b). Tying, of course, can constitute an antitrust violation. (Notably, Cablevision (which had been named as a respondent in DISH’s complaint) later sued Viacom in federal court, successfully alleging a claim that Viacom unlawfully “tied” it’s more popular channels to carriage of its less popular “suite” networks.xviii) By invoking Section 548(b), DISH may have sought to avoid the burdens of proving the technical requirements under the antitrust laws of separate products, relevant markets, and market power. The FCC also suggested, in 2007, that it might promulgate rules prohibiting program “tying” arrangements under its delegated authority to implement Section 548(b).xix

Whether and how “tying” of networks is actionable under Section 548(b) remains unclear. DISH and MSG settled their disputexx and the FCC did not engage in further rulemaking after soliciting comments on Section 548(b) “tying” claims. As MVPDs seek ways either to “slim” their bundles or price compete with new entrants, they may increasingly seek to claim that programmers are engaged in unfair “tying” practices. Conversely, new entrants may seek to invoke similar antitrust-ish theories to use Section 628(b) to attack Most Favored Nation provisions on the notion that the MFNs effectively prevent new entrants from gaining access to programming (because the programmer is unable or unwilling to incur the MFN “cost” to provide programming to the new entrant at a competitive price). A critical, and as yet unanswered, question is the extent to which the Program Access rules can go beyond the antitrust laws to restrain distributor conduct, but without violating the First Amendment under intermediate scrutiny. Indeed, the continued vitality of the Program Access regime largely rests on whether it allows the FCC to regulate from an antitrust “light” basis---an issue that has been, and will likely continue to be, hotly debated as the industry evolves.xoi

Endnotes:

i Cablevision Sys. Corp. v. FCC, 597 F.3d 1306, 1308 (D.C. Cir. 2010)
iii An interest of at least 5% is the principle determinant for whether a cable operator has an “attributable interest” in a programming vendor. 47 U.S.C. § 548(b).
iv Certain aspects of the Program Access regime also apply to “Satellite Broadcast Programming Vendors” regardless of whether they are affiliated with a cable operator or common carrier. E.g., 47 U.S.C. § 548(b).
v The FCC had confirmed that the Program Access rules will apply to the former DirecTV channels now acquired by AT&T. In re Applications of AT&T and DirecTV For Consent to Assign or Transfer Control of Licenses and Authorizations, 30 FCC Rcd. 9131,9194-95, 2015 WL 4556648 (FCC July 28, 2015).
vi An interest of at least 5% is the principle determinant for whether a cable operator has an “attributable interest” in a programming vendor. 47 C.F.R. § 76.1000(b).
A similar "temporary standstill" provision was promulgated under the Program Carriage regime in 2011, but vacated by the Second Circuit in 2013 for failure of the FCC to comply with the "notice and comment" requirements for rulemaking under the APA. *Time Warner Cable Inc. v. FCC, 729 F.3d 137 (2d Cir. 2013)*. The FCC has not reinstated a Program Carriage standstill provision.*

In re Am. Cable Co. and Jay Copeland, 11 FCC Rcd. 10090, 1996 WL 490244 (FCC Aug. 29, 1996). Accord In re Dakota Telecom, Inc., 14 FCC Rcd. 10500, 1999 WL 440407 (FCC July 1, 1999) ("Section [548(b)] cannot be converted into a tool that, on a per se basis, precludes cable operators from exercising competitive choices that Congress deemed legitimate.")


Compare In re Verizon Tel. Cos. v. Madison Square Garden, L.P., 26 FCC Rcd. 13145, para. 45 (Media Bureau Sept. 22 2011) ("Congress specifically adopted the program access regime, including Section 628(b), as a new remedy separate and apart from antitrust enforcement" and "that antitrust and program access laws address similar but not identical concerns.") and Cablevision Sys. Corp. v. FCC, 597 F.3d 1306, 1325 (D.C. Cir. 2010) Kavanaugh, J., dissenting (extension of ban on exclusive contracts violated First Amendment to the extent that concerns about exclusive contracts were inconsistent with antitrust laws).

---

The Forum on Entertainment and Sports Industries invites you to join one of its twelve (12) Forum Special Interest Divisions today! You can choose to be as involved as you like: from simply receiving information and updates to participating in online discussions and attending networking events. Enrich and enhance your experience in the Forum. **Join today!**

Get More Information on Forum Divisions

http://ambar.org/entertainmentsports
Looking Back at Sochi: Lessons from Putin’s Games

By John T. Wendt

The 2014 Sochi Winter Olympic Games, viewed as a triumph for Russian President Vladimir Putin for both landing the Games in Sochi and building a destination from scratch, can also be seen as a cautionary tale for future Games. The road to Sochi revealed many issues that must be addressed for future Olympics including the cost of preparing for the Games, political disputes having the effect of separating rather than unifying participating nations, selection of the Olympic events, ongoing drug concerns, and the safety of the athletes and spectators.

In only eight months, the 2016 Summer Olympics will be held in Rio de Janeiro, Brazil. Rio finds itself facing many of the same concerns that surfaced in Sochi with the three most prominent being Rio’s venue and infrastructure viability, the continued war on doping, and the call for greater transparency and reform in sports’ governing bodies. With this in mind, it is worth reflecting on the Games in Sochi to better understand the challenges the Olympic Games and its host nations continue to face.

Sochi’s Origins

On July 4, 2007 the International Olympic Committee (IOC) voted to select the host city for the 2014 Winter Olympic Games. In a surprise, first time bidder Sochi, Russia defeated favorites Salzburg, Austria and Pyeongchang, South Korea.[1] Russia never hosted a Winter Olympic Games and Sochi’s success was directly attributed to Putin. Putin personally delivered the presentation to the IOC in English and French, the languages of the Olympic Movement, and languages Putin rarely speaks. IOC member and former Olympic Champion Jean-Claude Killy explained that, “The Putin charisma can explain four votes.”[2] Sergey Mironov, Chairman of the Federation Council, the upper house of the Russian parliament, said that Sochi’s win was “a personal victory for Russia’s president.”[3]

In fact, it has been said that Sochi Olympics are “Putin’s Games.”[4] Not since the origins of the modern Games and founder Pierre de Coubertin has an Olympics been so closely identified with a single person.[5] Stephen Sestanovich, professor of international diplomacy at Columbia University, spoke of Putin saying that he is a “judo expert, and the games [sic] fit in with that, but they are also supposed to symbolize not just his role, but Russia’s reemergence on the international scene.”[6] Sergey Markedonov, visiting fellow in the Center for Strategic and International Studies Russia and Eurasia Program, said, “Putin considers the event to be a demonstration of Russia’s post-Soviet potential and its growing role on the international stage, as well as visible proof of his success in overcoming the political chaos that followed the dissolution of the USSR.”[7] For Putin, the Sochi Games would be the crowning symbol of Russia’s resurgence on the global stage. [8]

Much was made of the staggering cost of over $50 billion to hold the Games in Sochi. The amount spent in Russia was at least $10 billion more than was spent on the 2008 Summer Games held in Beijing.[9] IOC President Thomas Bach noted that after the dissolution of the Soviet Union, Russia, a winter sports country, was left without elite training facilities or venues to host world class events. Hosting the Games allowed them to build an Olympic site, elite facilities and rebuild a vacation destination from scratch. As Bach said, “I think this is a respectable interest and intention. And now we can see this winter sports center.”[10] About the $50 billion, Bach went on to say that it would be a long term investment, “You cannot [sic] just depreciate these investments in 17 days to zero.”[11]

Killy, Chairman of the Coordination Commission for the Games in Sochi, described the “unprecedented challenge” that Russia faced and how they overcame those challenges saying, “My first trip here was with the IOC president [Jacques Rogge] in September 2007, and there was nothing here except for promises. And these promises have been kept.”[12] However, the funds spent have gained the attention of the IOC and Bach has suggested that future bidders make greater efforts to control costs. [13]

International Olympic Committee Change of Leadership and Diversity

On September 10, 2013 Thomas Bach of Germany succeeded Jacques Rogge and became the ninth President of the International Olympic Committee. One of the first calls that Bach received was from Putin.[14] Bach’s manifesto was “Unity in Diversity” meaning “respect for different cultures, gender, social backgrounds, perceptions, attitudes and opinions . . . [and giving] a fair chance to each and every Member of our Olympic Family, re-gardless of gender, and to keep us free of discrimination of any kind.” [15]

However, one of the biggest diversity challenges that Bach immediately faced was the bill passed unanimously by the Russian parliament on June 11, 2013 banning the “propaganda of nontraditional sexual relations.”[16] Signing the bill, Putin said that Russia was defending traditional values and that “[i]n many countries today, moral and ethical norms are being reconsidered; national traditions, differences in nation and culture are being erased.”[17] Under the law individuals could be fined up to 5,000 rubles ($65) while media organizations could face a fine of up to 1 million rubles ($12,973).[18] Non-Russian citizens could also face deportation.[19]

According to the Rule 50 of the Olympic Charter, “[n]o kind of demonstration or political, religious or racial propaganda is permitted.”[20] Bach confirmed he received assurances from the Russian government that Rule 50 would be respected. Putin even stated that,
On my own and on your behalf, I have assured Mr. President (Bach) that we will do our best, and our athletes and fans will do their best too, so that both participants and guests feel themselves comfortable at Sochi Olympics regardless of their ethnicity, race or sexual orientation. I would like to underline that.

That was not enough for many human rights activists including Graeme Reid, LGBT rights program director at Human Rights Watch, who said, “Russia is trying very hard to make discrimination look respectable by calling it ‘tradition,’ but whatever term is used in the bill, it remains discrimination and a violation of the basic human rights of LGBT people.”

Jane Buchanan, associate director for Europe and Central Asia at Human Rights Watch went even further saying, “The Sochi Olympics risk being remembered as the anti-gay games, unless the IOC is willing to stand up and defend the principles of its own Olympic Charter.” The IOC said that, similar to the Games in Beijing, “protest zones” away from accredited areas would be provided where athletes would be free to speak their minds. This would allow compliance with Rule 50, respect the laws of the host country and allow free speech.

There were calls to boycott the Games similar to those of the 1980 Summer Games held in Moscow, when the United States protested the Soviet presence in Afghanistan. History has shown that boycotts, such as President Carter’s in 1980, rarely work. While in Sochi there would be no boycott preventing U.S. athletes from attending, President Obama decided that there would be an “Administration Boycott” where neither he, the First Lady, nor any member of his cabinet would go.

This was the first time in six Olympic Games that the president, vice-president or a former president was not a member of the U.S. delegation for the opening ceremony.

President Obama stated, “Nobody is more offended than me by some of the anti-gay and lesbian legislation that you’ve been seeing in Russia.” So instead of attending the Games in Sochi himself, President Obama named two openly gay athletes, tennis star Billie Jean-King and figure skating star Brian Boitano to the U.S. delegation. He was not the only leader boycotting as Germany’s Angela Merkel, France’s François Hollande and Canada’s Stephen Harper all stayed away. British Prime Minister David Cameron sent British Sports and Equalities Minister Helen Grant in his place. Surprisingly, the Dutch, who are outspoken supporters for gay rights, sent King Willem-Alexander and Queen Máxima, as well as their prime minister and sports minister. Prince Albert of Monaco, Italian Prime Minister Enrico Letta and Japanese Prime Minister Shinzo Abe also attended. In fact over thirty heads of state, nearly twenty heads of government and fifty-eight ministers of sport attended. This was three times the number of leaders who made it to the 2010 Vancouver Games, and a Winter Games record.

Russian Foreign Minister Sergei Lavrov said that heads of state that chose not to attend the Games had, “rejected an invitation from the International Olympic Committee, and not from Russia.”

The decisions to not attend the Games did not go unnoticed by the IOC. Bach has constantly stressed Nelson Mandela’s words that “Sport can change the world” and that, “We are grateful to those who respect the fact that sport can only contribute to development and peace if it is not used as a stage for political dissent or for trying to score points in internal or external political contests. To other political leaders we say: please understand what our responsibilities are and what your responsibilities are. Have the courage to address your disagreements in a peaceful direct political dialogue and not on the backs of the athletes.”

During the Games, it seemed that the controversial anti-gay legislation became a non-issue. Austria ski-jumper and silver medalist Daniela Iraschko-Stolz, who married partner Isabel Stolz last year, said, “I don’t think it’s a good idea to make protests here, no one cares . . . I know Russia will go and make the right steps in the future and we should give them time.”

Security at the Games

Security in Sochi was also a major issue. In December 2013, a little more than a month before the start of the Games, terrorists launched devastating suicide attacks at the Volgograd railroad station, a major transportation hub approximately 400 miles northeast of Sochi. It is believed that the attacks came from separatist terrorists based in the North Caucasus area, including Chechnya. Bach said, “This is a despicable attack on innocent people and the entire Olympic Movement joins me in utterly condemning this cowardly act . . . The Olympic Games are about bringing people from all backgrounds and beliefs together to overcome our differences in a peaceful way.”

Following the attacks, the U.S. State Department issued travel alerts warning Americans travelling to Sochi. Bill Rathburn, who directed security at the 1996 Summer Games in Atlanta said, “It’s not a matter of whether there will be some incident, it’s just a matter of how bad it’s going to be.”

US Representative Mike McCaul, Chairman of the House Homeland Security Committee, said, “What poses the greatest threat, in my opinion, is the proximity and the location of where these games are being held. It’s a whole new ball game, makes these Olympics very, very different. I think there’s a high degree of probability that something will detonate, something will go off.”

There were concerns that female suicide bombers, known as “black widows”, would infiltrate the Games, in addition to worries that toothpaste containers containing bomb-making materials would be used to bring down commercial planes.

In the event of a security emergency, two U.S. Navy warships were deployed to the Black Sea. Two additional destroyers were deployed in the Mediterranean that could also quickly sail to the Black Sea. The U.S. European Command also placed several transport aircraft, helicopters, fixed-wing aircraft and troops at bases in Great Britain, Germany and elsewhere that could rapidly assist with evacuation efforts. In Russia, Putin promised to create a “Ring of Steel” to protect athletes and fans. Reportedly, Putin spent $2 billion in security at the games while deploying 40,000 troops around Sochi.
In the end there were no reported major security issues at the Games and many wondered if the threats were overblown. Before the Games the U.S. Ski and Snowboard Association hired Global Rescue to provide medical and security support in case of an emergency in Sochi.[43] Even though no major events occurred, Global Rescue CEO Dan Richards stressed the importance of a risk management plan saying, "Maybe there was a little unnecessary sensationalizing, but the fact remains this is an area of the world that has risks associated with an Olympics that didn’t exist in previous Olympics, so having an additional level of scrutiny and concern was justified." [44]

New Sports and Athlete Safety

Twelve new sports made their debuts in Sochi.[45] When selecting a new event for the Games, the IOC Olympic Programme Commission analyzes all the requests put forward by the International Sports Federations in terms of universality, gender equity, youth appeal, and added value to the Games. Former IOC President Jacques Rogge said that the new events, "provide great entertainment for the spectators and add further youthful appeal to our already action-packed lineup of Olympic winter sports."[46] Bach has said that adding new events is a "balance between tradition and progress" and has "encouraged" other sports to modernize their competition without compromising their fundamental cores.[47] U.S. snowboarder and 2006 silver medalist Gretchen Bleiler said, "I think the Olympics needed this energy…The Olympics looked at ESPN’s X Games and saw the enormous popularity, and they wanted in on something that was new, exciting and fresh."[48] Many of the new events were inspired by the X Games.

Three new mixed events were introduced in Sochi. The biathlon mixed relay is comprised of two men skiing and shooting targets over a distance of 7.5km and two women skiing and shooting targets over a 6km distance. The figure skating team event, with each team comprised of one male, one female, one pair and one ice dance couple, is a competition where points are awarded for each routine, and the team with the highest aggregated score is the winner. The mixed luge team relay includes a men’s singles sled, a doubles sled and a women’s singles sled. Each sled slides one after the other as teams compete for the fastest combined time.

New individual events at the Games included men’s and women’s ski halfpipe, men’s and women’s ski and snowboard slopestyle, where skiers and snowboarders select their own line through a course of rails, boxes and a variety of jumps before being scored on execution, style, difficulty, variety and progression, and women’s ski jumping.

The women ski jumpers had been lobbying for many years for inclusion into the Games, but had found the door closed. They were denied on a number of grounds including their health and “universality,” or support within the international community. At the 2010 Olympic Games several jumpers filed suit against Vancouver Organizing Committee charging a violation of Canada’s Charter of Rights and Freedoms which bars gender-based discrimination. While British Columbia Supreme Court Justice Fenlon found that there was discrimination against the women according to the Charter, the Charter did not apply to the IOC.[49] “The IOC made a decision that discriminates against the plaintiffs. Only the IOC can alleviate that discrimination by including an Olympic ski jumping event for women in the 2010 Games.”[50] The IOC finally agreed to allow women to ski jump in Sochi. Still, while men competed in three events, on the “normal hill” (K95), large hill (K125) and a team event, women jumpers were limited to one event on the “normal hill” (K95). [51]

Despite the “X Games energy,” spectator appeal and desire to get good television ratings, the safety of the athletes should still be paramount in the minds of the Games organizers. This is especially true since the death of Georgian luger Nodar Kumaritashvili the 2010 Vancouver Games. For Sochi, the designers modified the luge track so that the maximum speed was lowered from approximately 100 to 75 miles per hour. [52] But slower did not mean less technical and the course proved challenging for the athletes. [53] Georg Hackl, a three-time gold medalist and current coach said, “It’s difficult to have a fast time…But it’s not dangerous. That’s the important thing.”[54] In fact, Romanians Radu Sovaiala and Alexandru Teodorescu, who crashed during a training run, were barred from starting the Olympic luge doubles competition because the International Luge Federation (FIL) said it would be too dangerous for them to compete.[55]

The luge was not the only event where there were safety issues. American Jacqueline Hernandez and Norway’s Helen Olafsen had to be carried off the snowboard course after suffering injuries. Hernandez was knocked unconscious and was motionless on the ground before medical personnel carried her off the course on a sled. After one jump, Olafsen turned 180 degrees before landing on her back and shoulder and lay on the course with torn ligaments in her knee. Germany’s Anna Woerner was carried off the skicross course on a stretcher after a knee injury. The most serious injury at Sochi was to Russian skicross racer Maria Komissarova, who crashed during a training run, was barred from starting the Olympic luge course because the International Luge Federation (FIL) said it would be too dangerous for them to compete.[55]

The women’s super-G downhill was called “disaster” by many of the competitors. [57] Only one of the first eight starters, and 31 of 49 athletes who started, finished the course. Switzerland’s Laura Gut, who finished fourth overall said, “This is a disaster, it was a shame for everybody… It’s not a race. You are just trying to come down.”[58] Three-time Olympic champion Maria Hœfl-Riesch of Germany, who won the super-combined and was silver medalist in the super-G said, “This shouldn’t happen, because it’s dangerous.”[59]

Perhaps the biggest issue was the high amount of injuries in slopestyle. Many of the competitors, including defending champion American Shaun White and Australian Torah Bright, criticized the design of the slopestyle course.[60] White, the sport’s biggest star, withdrew from competition saying that “even after course modifications and watching fellow athletes get hurt, the potential risk of injury is a bit too much for me to gamble my other Olympics goals on.”[61] Norwegian snowboarder Torstein Horgmo, who broke his collarbone in a practice run said, “Injuries and falls are
part of this sport, but the timing is really bad.”[62] Other injuries included Rowan Cheshire of Great Britain and Marika Enne of Finland both suffering concussions, Norwegian Kjersti Buaas’ violent fall resulting in her slamming face first into the snow and Sarka Pancochova of the Czech Republic crashing so hard that she cracked her helmet and lay motionless until medics arrived.[63]

The slopestyle course design was put together with help from officials who worked on the courses for the X Games.[64] Development Snowparks, which built the pipe, admitted that the pipe was not up to its standard.[65] But Snowparks CEO John Melville denied any possible liability. Snowparks said it left the pipe in a safe condition and was not responsible for its deterioration saying, “It’s the job of FIS and running the competition that look after the safety while the competition is running, and that’s always high on their agenda.”[66]

In 2010, the IOC commissioned an examination of injuries at the 2010 Games at Vancouver.[67] The main findings were that at least eleven percent of the athletes suffered an injury during those Games, with snowboarding the most hazardous with about thirty-five percent of the athletes getting hurt.[68] International Skiing Federation secretary general Sarah Lewis commented the injuries at Sochi saying, “Ultimately, there will be accidents…These things are a hazard of the competition.”[69]

Snowcross athletes appear to have an aura of invincibility. In 2005 alone, Zoe Gillings of Great Britain broke all the bones in the middle of her left foot, tore ligaments in her knees and shoulders, tore cartilage in her knee, broke both collarbones and had six concussions. Yet, Gillings said she keeps going. “When you race, the fact you’re hurting 50 mph down a hill and going off massive jumps, that danger doesn’t fit into your brain.”[70] By the time he was 20-years-old, American snowboarder Trevor Jacob admitted that he has had over 25 concussions.[71] Jacob went on to say, “But yeah, whatever…It comes with our lifestyle. If you don’t accept it, you’re kind of doing the wrong thing.”[72]

The question is in making the Games more youthful, more exciting and even more extreme are the organizers placing the athletes at greater risks? For example, in snowcross, unlike the past two Winter Olympics where there were four athletes per heat, Sochi’s event had six athletes in each heat. US athlete Nick Baumgartner said, “I think it is more dangerous…It’s more exiting. It changes it. Anything can happen. It’s totally unpredictable when you’re going down the course.”[73] Baumgartner continued, “If it’s dangerous and scary and I overcome it and I do well, that’s what I’m looking for: that adrenaline, that rush… So add more people, make it even scarier, because that’s what I’m here for. I want to have some fun with it and enjoy it.”[74] Following Sochi, questions remain. Will there come to a point where the events become too dangerous? Is the increasing number of injuries acceptable?

**The Fight Against Doping**

The anti-doping program at Sochi was one of the most stringent in history with over 2,600 tests conducted at a cost of approximately one million dollars.[75] The number of out-of-competition doping tests was up sixty percent over tests conducted in Vancouver.[76] To keep up with ever-changing doping techniques, athletes’ samples will now be kept for ten years. Article 17 of the new version of the World Anti-Doping Code allows for a ten-year statute of limitations.[77] Arne Lundquist, the IOC medical commission chairman, said that the message is that, “If you cheat, if you take drugs, even if we don’t catch you now we will certainly catch you sooner or later.”[78]

While at Sochi, seven athletes tested positive for prohibited substances, and most involved stimulants that are found in food supplements. Because they are considered “specified substances” they are considered more susceptible to inadvertent use and may result in reduced penalties. Three athletes tested positive for methylhexanamine; two-time Olympic cross-country champion Evi Sachenbacher-Stehle of Germany, who finished fourth in two biathlon events in Sochi; [79] Italian bobsleigh brakeman William Frullani, who claimed his positive test solely due to nutritional supplements; [80] and Vitalijis Pavlovs of Latvia who admitted taking supplements on the advice of his club team doctor. [81] Ukrainian cross-country skier Marina Lisogor tested positive for trimetazidine, prescribed by a cardiologist (who was not associated with the Ukrainian National Olympic Committee) for fatigue thought to be due to her hypothyroid condition.[82] Polish bobsledder Daniel Zalewski was banned for the stimulant phenethylamine which is found in the sports pre-workout supplement, Craze.[83] And though his teammates had done nothing wrong, because Zalewski tested positive, the entire four-man bobsleigh team was disqualified.[84]

Swedish hockey star Nicklas Bäckström tested positive for pseudoephedrine in excess of the acceptable limits and was suspended just before championship game between Sweden and Canada. However, the IOC Disciplinary Committee later found that he had declared the medication on the doping control form and there was also no indication that he had taken the medication for performance enhancement.[85] Bäckström was subsequently awarded a silver medal.[86]

The Games’ biggest disappointment was Austrian cross-country skier Johannes Duerr who tested positive for erythropoietin (EPO), a banned performance enhancing substance. EPO is used to boost an athlete’s count of red blood cells, which carry oxygen to the muscles, increasing stamina and endurance. Duerr apologized saying, “So many people worked their butts off for me and I disappointed them with my stupidity. First of all I would simply like to apologise and everything else, all further steps, we’ll see what comes my way. I don’t know myself yet.”[87] Markus Gandler, Austria’s director for biathlon and cross-country, expressed the anger the team felt saying, “This is the worst thing that I could not even dream about. The team is broken…We ripped our asses off for this dog and then you get deceived in this way. I’m sorry for the team that we had such a scoundrel.”[88] Subsequently on April 9, 2014 the IOC formally disqualified both Duerr[89] and Zalewski.[90]
The Court of Arbitration for Sport at Sochi

Beginning in 1996 the Court of Arbitration for Sport (CAS) has had special tribunals, called the CAS ad hoc Division that operate at both the Winter and Summer Olympic Games as well as the FIFA World Cup and the Commonwealth Games. The ad hoc Division is designed to provide expedited hearings and the Panels of the ad hoc Division will generally render their decisions within 24 hours, critical to an athlete’s ability to compete in the Games. The Panels are usually composed of three arbitrators, athletes are not required to pay any fees for their dispute to be resolved and the Panels judgments are normally final and without appeal. Their motto is “Fast, Free and Fair.” At Sochi the ad hoc Division heard five cases.

Austrian halfpipe skier Daniela Bauer asked the CAS ad hoc Panel to order the Austrian Ski Federation (ASF) and the Austrian Olympic Committee (AOC) to place her on the Austrian Olympic team in the women’s freestyle ski halfpipe. Bauer claimed that she had met all the FIS qualification requirements and had several top-20 performances that year on the World Cup circuit. Although Austria secured a quota position, ASF decided to not select anyone for the women’s halfpipe because they felt that Bauer was not “adequately prepared for high level international competition …” a requirement of Rule 44.5 of the Olympic Charter. The CAS Panel rejected Bauer’s application finding that Austria’s decision not to nominate an athlete in the halfpipe was not arbitrary or capricious, but rather that the ASF had a legitimate sports performance justification for not recommending her nomination. The Panel did criticize ASF for a “lack of published qualification criteria [which] has misled the athlete.”

Clyde Getty was a 52-year-old Argentinean aerial skier who had participated in the Olympic Winter Games in 2002 and 2006. Getty requested the Panel to order the Argentinean Olympic Committee to enter him into his third Games. Getty argued that he was eligible because the international governing body, Fédération Internationale de Ski (FIS) had allocated a quota place to the National Olympic Committee of Argentina (COA) and he was the next person eligible. The FIS replied that the quota was given erroneously and that Getty did not meet the minimal qualifications. The Panel agreed with the FIS and, while acknowledging Getty’s “illustrious career,” rejected his application.

Maria Belen Simari Birkner, an Argentinean skier, requested the CAS ad hoc Division Panel to order the Argentinean Olympic Committee to enter her in slalom, super-G and giant slalom events. She alleged that her non-selection was arbitrary and capricious and caused by discrimination against her and her family. She claimed that her family was legendary and had dominated Argentinean Alpine Skiing for over 30 years, and that the Committee had discriminated against her on the basis of her family affiliation, a form of discrimination prohibited by the Olympic Charter and Fundamental Principles of Olympism. The CAS Panel found that it had no jurisdiction because the dispute arose before the date of the Panel’s jurisdiction started to be effective. Nonetheless, the Panel did discuss the merits and found that the athlete failed to establish discrimination, especially since other members of her family were chosen to participate in Sochi. However, the Panel did criticize the Argentinean ski federation and recommended that they establish clearer selection criteria in the future for their athletes.

In the Men’s Ski Cross event, the top three finishers were all from France. Alpine Canada Alpin (ACA), the Canadian Olympic Committee (COC) and the Slovenian Olympic Committee (SOC) all asked the International Ski Federation (FIS) Competition Jury to disqualify the French athletes because, they alleged, the French support staff had changed the shape of the athletes’ suits to make them more aerodynamically efficient, contrary to FIS rules. However, FIS rules stipulate that protests must be filled within fifteen minutes of the completion of the last competition run of that phase of the event. The ACA and COC did not file their protests until six hours later and the FIS Competition Jury denied their protest. The Panel noted the ACA, COC and SOC all knew of the French design at the time of the race that there were no extenuating circumstances in the protest delay and denied their appeal.

Nationality Changes and Scoring Controversies

Nationality changes were noted at the Games. At Sochi, Viktor Ahn became the most decorated short track speed skater in history and did so for two different countries. Competing under his original name Ahn Hyun-soo, Ahn won four medals at the 2006 Games in Torino for South Korea; gold in the 1000m, 1500m and the 5000m and a bronze in the 500m. Following Torino, injuries kept him from competition and Ahn did not qualify for the 2010 Games in Vancouver. Ahn felt that other South Korean skaters were given preferential treatment, and after bitter fallout with South Korean officials, Ahn looked for support from another country. Viktor Ahn, Russia, which had won only one short track medal in the past, became a powerhouse overnight. In the 1,000m Ahn won gold and teammate Vladimir Grigorev, who competed for Ukraine at the past two Games, claimed silver.

In a similar vein, five years ago U.S. born snowboarder Vic Wild moved to Moscow to marry Russian snowboarder Alena Zavarzina. He, too, complained about the lack of support, this time from the U.S. Ski and Snowboard Association, which poured more resources into the halfpipe and slopestyle, than his event in slalom. As Wild explained it, “I’m not like some dude that lives in the United States and decides, ‘Oh, man, it’ll be easy for me to go to the Olympics and go to some country that doesn’t do anything.’ Some country that doesn’t have any athletes. I went the hard way. Russia has lots of good riders.”
Wild won gold for Russia in the men’s parallel slalom and men’s parallel giant slalom. His wife, Alena Zavarzina won the bronze in the women’s parallel giant slalom.

Concerns over scoring in ice skating continued in Sochi. At the 2002 Olympic Games in Salt Lake City there were allegations that the Pairs competition was “fixed.” Judges were reprimanded and the scoring system was revamped. At Sochi, in ice dancing, there was controversy in the short program when Canadian pair Tessa Virtue and Scott Moir, the defending Olympic champions, finished more than 2.5 points behind rivals Charlie White and Meryl Davis of the U.S. It was questioned in part because one of the judges marked Virtue and Moir down on an essential dance element called the “Finnstep.” Moir described it as, “(A) 36-second segment where all the skaters have to do the same step in the same hold and they judge six specific (factors) very crucially. And it’s worth a lot of points. That’s where you make it or break it in this dance.”[103]

The biggest controversy occurred in judging women’s figure skating, where Adelina Sotnikova of Russia upset defending champion Yuna Kim of South Korea. It was the first time that a Russian woman had won the women’s event. Yuna Kim led after the short program and both skated flawless long programs, but Sotnikova won the long program by 5.48 points, a very large amount in skating.[105] Controversy arose not only because Sotnikova won, but also due to her margin of victory. Prior to her victory in Sochi, Sotnikova had never won a Grand Prix event, nor had she even medaled at a major senior international competition. [106] Her gold medal winning score was eighteen points higher than she had ever achieved before, more than eight points higher than any other skater scored in the past year, [107] and was the second highest score in history behind only Kim’s at the 2010 Vancouver Games.[108]

The attention immediately turned to the judges and the composition of the judging panels. One of the recommendations enacted after the 2002 Olympic Games skating scandal was to make the judges’ scores anonymous. Therefore, while it is difficult to focus on any one individual judge, there can be questions about the composition of the judging panel.

Alina Shekhovtseva served on the women’s figure skating judging panel. She is married to Valentin Piseev, the president and general director of the Russian Skating Federation. Shekhovtseva was seen hugging Sotnikova immediately after the results were announced.[109] Another member of the panel was Ukranian Yuri Balkov, who was suspended for one year when he was tape-recorded trying to fix the ice dancing competition at the Olympics in Nagano in 1998.[110] Ottavio Cinquanta, president of the International Skating Union (ISU) saw no issue saying, “Would you rather have an idiot acting as a judge than a good one who is a relative of the manager of a federation? It is far more important to have a good judge than a possible conflict of interest.”[111]

American Scott Hamilton, 1984 Olympic champion and a television analyst, said that the problem was not with the scoring system, but rather, “[How] the judges are selected for these competitions…Every sport out there has an affiliated association of officials. They are separate from the federation, and figure skating is hesitant to do that. It is a fundamental issue that leads to people having a hard time taking the results as the results.”[112]

The ISU rules allow complaints to be filed within sixty days of the event, and in late March of 2014 officials at the Korean Olympic Committee and the Korea Skating Union said that they would file a complaint.[113] They asked the ISU for an investigation into the judging in the women’s competition claiming that the judging was “unreasonable and unfair.”[114] According to reports, the complaint alleged violations of the IOC Code of Ethics based on the presence of both Shekhovtseva and Balkov and on “suspicions of bias by other judges.”[115] Cinquanta said that there must be evidence of wrongdoing, but also acknowledged that the ISU must make the system more transparent and understandable saying, “We have to convey, give an explanation that is clear to everybody.”[116]

**Conclusion**

From Russia’s viewpoint the Games in Sochi have to be viewed as a success with its resurgence on the global stage. Former IOC marketing director Michael Payne said the Sochi Games “will be a case study in expectation management. People came here with concerns and they didn’t materialize. From an operational perspective or the key things that matter, it’s as good as it gets.”[117] More than 225 miles of roads and bridges, 125 miles of railway and 400 miles of utilities were built ahead of the Games.[118] From a spectator’s point of view the Olympic site was incredibly compact. Attendees could walk to multiple events the same day. The trip from the shoreline venues to the mountain venues was only 45 minutes. Buses and trains ran on time. The security lines that were endless in Beijing were quick and efficient in Sochi with most spectators going through security in about thirty seconds.[119]

The terrorist attacks that prevented many from attending did not materialize, nor were there significant boycotts. There were no high-profile, provocative statements or blatant symbolic gestures by athletes regarding Russia’s anti-gay legislation. There were some difficulties, especially with housing and hotels. Some hotels were never finished and some rooms did not have phones or other amenities, such as shower curtains. Terrence Burns, a managing partner with Teneo Holdings and a consultant on Sochi’s bid to host the Games, said the Russians “did it their way, as any country does….Think about building a city in seven years. There are only two countries that can do that — Russia and China. They said we want the Games, we’ll deliver it, and they did it.”[120]
Sadly, shortly after the Olympic Games ended and before the Paralympics began, Russia's parliament gave Putin permission to deploy troops into Crimea and said that they should remain there until the "political-social situation in the country is normalized."[121] The actions in Crimea created a long shadow on the Paralympic Games. The Crimean capital, Simferopol is only 300 miles southeast of Sochi. Again, some called for boycotts of the Paralympic Games.[122] Ukrainian athletes refrained from boycotting, but made symbolic gestures. At the opening ceremony, the sole representative of Ukraine was flagbearer Mykhaylo Tkachenko and Ukrainian athletes covered their medal during awards ceremonies.[123] Iuliia Batenkova, a Ukrainian biathlon and cross country star said, "That is how we show our protest and disagreement that our country could be divided and part of it could be excluded from Ukraine…Crimea is my motherland, where I was born, and of course I worry about it. I want peace."[124]

Despite the political unrest, Russia welcomed and celebrated the Paralympics. The Games were attended by a record 597 athletes from 45 countries and a record 287,000 tickets were sold compared to the 57,000 tickets sold in Vancouver. [125] International Paralympic Committee (IPC) president Sir Philip Craven said, "The Games have been absolutely mind-blowing (sic) in terms of their impact, far beyond what the Paralympic movement expected when coming here . . . They have been a spectacular showcase of sport and the power of the human spirit. Not only have the athletic performances been first class, but so has the organization, which has been seamless."[126]

After the Paralympic Games, Vladimir Putin was invited to visit the IOC headquarters in Switzerland provoking even more controversy amid widespread condemnation of the situation in Crimea. IOC spokesman Mark Adams explained that the invitation was purely "protocol" which happens after every Games, and similar to the invitation extended to Britain's Prime Minister David Cameron after the 2012 Olympic Games in London. Putin indicated he planned to take up the IOC on its offer. [127]

Finally, Rule 2, Article 14 of the Olympic Charter states that an important role of the IOC is "to promote a positive legacy from the Olympic Games to the host cities and host countries."[128] Russia created, at a substantial cost, both an Olympic city and a destination winter resort from scratch. The site was the most compact site in modern Olympic history. Dmitry Chernyshenko, president of Sochi's organizing committee, said, "We have created a fantastic cumulative effect that united the nation and turned dramatically the attitude from abroad to Russia . . . We delivered what we have promised."[129] Killy said, "In Europe you would probably spend 15 years on that, and here they did it in seven . . . All of the promises made in 2007 have been kept and spectacularly so . . . It's a new city that's going to organize these games and show itself to the world - a city that is reflecting the new Russia."[130]

What will be the legacy of the Games in Sochi? For the tangibles, the sites will be used as national training centers for Russia's athletes as well as National, International and World Championships. The stadium will be used for games at the 2018 World Cup and there will be a Formula One Auto Racing Circuit from 2014 to 2020.[131] There is hope Sochi will grow as an international resort destination. At the Vancouver Games Russia earned only three gold medals and just fifteen overall. At Sochi they earned thirty-three medals, the most of any nation; thirteen were gold, eleven silver and nine bronze. It was the first time that Russia has been atop the medal table since the dissolution of the Soviet Union. The intangibles of the 2014 Sochi games enhanced Putin's stature at home and it achieved Putin's vision to reinvent Russia's image and place them back on the world stage. As noted journalist Alan Abrahamson said, "The Russian president, Vladimir Putin, bet big on these Games. And he has won his bet."[132]

Endnotes

[3] Id.
[5] Id.
[6] Id.
Takeaways from the Sony Pictures Entertainment Hack

By Maia T. Spilman

November 2014 Sony Pictures Entertainment (“Sony” or “SPE”) was paralyzed for several days by one of the biggest hacking incidents to date. The film and production company remains in business and the apparent damage as of this writing seems quantifiable. So, what can others learn from Sony’s “misfortunes” if the company seems to be doing fine? A few things are educational about the incident:

- The entertainment industry is not immune from breaches, hacks and leaked information. Even if this business sector is not legally required to implement privacy and security measures, it cannot dismiss such measures out of hand.
- Preventative measures aren’t sexy, interesting or prioritized but, they probably cost less than the approximate $42 million the breach reportedly cost Sony thus far (not including litigation costs).
- Bad publicity may not bring down a big company or a project but certain careless practices can impact individuals, careers, and tarnish a company’s long-term credibility.
- Entertainment companies biggest assets are its intellectual properties; copyrights, trademarks, trade secrets and patents. These assets are worthy of protection. Data, personal data, while not quite intellectual property, is another asset worthy of protection.

This article looks at some of the basic practices that Sony Pictures Entertainment could have had in place that would probably have limited the initially devastating impact of the November 2014 hack.


On Monday, November 24, 2015 computer screens at Sony Pictures Entertainment were rendered useless. All the computers would do was display an ominous message stating they’d been hacked by GOP (Guardians of Peace) with an image of a skull and a warning to obey or all internal data would be displayed to the world. That was the beginning.

The subsequent events, themselves worthy of a film, unfolded bit by painful bit over the next four weeks making headlines through Christmas day. Here’s a brief synopsis of some of the highlights in between and for a few weeks following the holiday.
Sony's computers, emails and voicemails were out for at least 5 five days.
Malware injected into the network erased data on the corporate servers and even erased computer operating systems, wiping out half of the company's global network (including over 800 of its servers).
100 terabytes of data were stolen from Sony, over several weeks 7-9 separate data dumps of personal, confidential, proprietary, medical and embarrassing information were leaked onto file-sharing and public sites including the following:
- Salaries of 6,000 current & former employees including executives (and 30,000 employees of consulting firm Deloitte)
- 47,000 Social Security Numbers
- Passport and visa information of cast and crew
- Film budgets
- Confidential agreements
- Passwords and user names for executives
- Dump of full emails of top executives Amy Pascal & Michael Lynton
- List of celebrity aliases
- Medical records of employees
- HR information including dates of birth, medical costs of some employees and their families
- Five films were dumped onto file-sharing sites; four which had not yet been released [1]
- Script for James Bond film then in production
- Sony employees were threatened with harm to themselves and their families if they did not sign a statement renouncing Sony and its practices.
- The FBI begins an investigation.
- Sony hired a cyber expert to investigate.
- Sony hired David Boise to threaten media outlets reporting on the data dumps or using the data dumps in their reporting.
- Two class actions lawsuits were filed by current and former employees accusing Sony of improperly protecting their personal information (in total more than 7 such suits were brought against Sony).
- The hackers threaten 9/11 style attacks on movie theaters that show the “Interview” (the film blamed as the root cause of the hack).
- The White House said this is a serious national security issue requiring a tempered response.
- The White House imposed economic sanctions against North Korea which it and the FBI claimed were behind the hack.
- Major theater chains pulled out of showing the film on its scheduled Christmas Day release.
- Sony pulled the release of the “Interview” on Christmas day.
- Presidential Obama criticized Sony for “caving in to” terrorists threats.
- The White House said North Korea should compensate Sony for its damage.
- Sony announced the “Interview” will be available via Video on Demand on a handful of platforms and available for screening to those theaters (mostly independents) who wanted to screen it. [2]

**Intentional Hack**

It is true that the Sony hack was more than just an ordinary breach of its systems and information. From all accounts, this was a deliberate, malicious attack specifically intended to harm Sony. It is likely that no measures could have prevented this deliberate hack. But it is probable that the extent of the damage could have been limited if Sony’s practices included some basic measures.

**Hack and breach are used interchangeably in this article but, there is a difference.**

A breach is any situation in which sensitive or confidential information is potentially accessed by someone who does not have authorization to view or use the information. Wikipedia defines a data breach as:

“a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal [protected] health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property.” [3]

A common example of a breach is an instance when an employee loses a laptop containing sensitive information or accidentally sends an email to the wrong person that has the personal or sensitive information of a third party or a company’s confidential or proprietary information.

A hack on the other hand is an intentional break in to computers or computer networks by someone not authorized to do so. According to Oxford Dictionaries in the context of information hack means:
“gain unauthorized access to data in a system or computer.” [4]

Most companies have experienced some type of breach or hack. They may not openly discuss it or they may not be aware of it. There is an adage in the privacy and cyber-security community: “There are two types of companies; those that have been hacked and those that don’t know it yet.” For most companies, it takes well over six months to learn they’ve been breached and nearly 70 percent of companies learn that they have been hacked by a third party such as the FBI.[5] If someone really wants to break into your client’s network, as the Sony hack seems to indicate, there is a good chance they will. And, there is also a good chance your client can thwart the extent of the damage caused, even if Sony did not.

Security experts do not think the security at Sony was particularly robust. Fortune Magazine published an extensive 3 part series by Peter Elkind in July 2015 which included an interview with:

“Ed Skoudis, a ‘white hat’ hacker who teaches cyberdefense testing for corporate IT security professionals at the SANS Institute, says the skill level deployed at Sony looks ‘pretty average.’ He puts its perpetrators on par with students in his mid-level classes. ‘It shows the defenses of Sony were not particularly good,’ says Skoudis. ‘I didn’t see the bad guys jumping over any extreme hurdles, because there weren’t any extreme hurdles in place.’” [6]

Legal Requirements

Probably the biggest take away from the Sony hack is that the entertainment industry is not immune from hacks, breaches and cyber-security threats. That’s right, even the freewheeling, cavalier minded entertainment industry is vulnerable. It’s safe to say that like Sony (pre November 2014), most entertainment companies have not prioritized privacy and cyber-security measures. And, why should they? After all, no law requires pro-active privacy and security measures in this business and, until Sony, all was quiet on the entertainment front. Frankly, no one wants to plan and budget for something that MAY happen if not required to do so. Before examining why implementing best practices for confidential, personal and proprietary data is probably a good thing, here is a quick look at the U.S. privacy law landscape.

At the moment in the U.S. there is not one centralized federal law regulating the use of personal data. Instead, we mostly have a sector-based approach to privacy. Only certain companies in the financial services industry (subject to Gramm Leach Billey “GLB”) and in the healthcare industry (subject to Health Insurance Portability and Accountability Act “HIPAA” and Health Information Technology for Electronic and Clinical Health “HITECH”) have an affirmative obligation to protect and secure individuals’ personal data. In addition to sector-based laws, the U.S. has a variety of federal and state laws that contain privacy components or otherwise address some aspect of handling individuals’ personal information. Examples include: the Fair Credit Reporting Act (“FCRA”), the Children’s Online Privacy Protection Act (“COPPA”) and “CAN-SPAM” (the acronym represents Controlling the Assault of Non-Solicited Pornography and Marketing). All industries, including entertainment, must take certain measures when obtaining a credit report (FCRA), marketing to children online, or even suspecting that children visit their website (COPPA) and sending marketing emails/newsletters (CAN-SPAM). So, that even entertainment companies must comply with some “privacy” laws.

Under U.S. law no entertainment company is required to encrypt personal data, or any data. Among the items stolen from Sony in the hacking incident and posted for all the world to see and use were; employee and contractors payroll information, addresses, social security numbers, dates of birth, and passport and visa information of certain cast and crew. All this type of personal information or data is ripe for identity theft; not just credit fraud. [7]

While GLB, HIPAA and HITECH, all of which require special treatment of such information, may not directly apply to Sony, best practices make clear that this type of personal information should not be sitting openly in clear text on a server. Companies of all sizes who have employee or contractor personal data[8] will be well advised to treat this type of information with greater care. At a minimum such personally identifiable information should be secured (encryption is best) and should be accessible only by those individuals within the company who need this information to fulfill their job function. Apart from federal law, states have their own breach notification laws. In these, if specific information is breached, notice has to be given to government officials as well as individuals. In order to comply with these laws, companies will want to be pro-active about individuals’ personal data. More on breach notice in Lesson #6 below.

Note that in other jurisdictions, Europe in particular, there are specific laws on how to handle personal data. Data protection laws in the EU are generally more protective of the individual than the variety of privacy laws in the U.S. EU data protection laws are currently being revised and further strengthened. In an increasingly globalized and electronic world, understanding laws affecting data of all jurisdictions will play a greater role in business. Thus having an understanding of your client’s data, and how it flows into, through and out of the organization including who accesses it along the way, proves valuable in a global context as well.

Securing Data and Intellectual Property

At least seven class action lawsuits were filed against Sony by current and former employees for the company’s failure to protect their personal information. Whether Sony had a legal obligation to protect that information may never be
determined. Sony is not directly subject to the laws requiring a heightened level of protection for certain types of information and, at the time of this writing, there were reports of joining all of the actions into one and of a settlement being near. Regardless of the resolution and potential settlement sum, Sony has had to spend time and resources responding to these actions. The financial cost is real. Companies which are smaller than Sony may not be in a position to shoulder employee and consumer actions.

There is another cost for not treating personal information with care; employees and prospective employees may not find your client’s shop to be a desirable place to work. Who wants to work for a place that handles your personal information carelessly and potentially jeopardizes your identity? For some companies doing the “right” thing may not outweigh the costs of implementing certain measures or the perceived inconvenience of tightened security. Each company has to determine what is most suitable for its circumstances however, the desirability of your client’s organization as a place of employment is one factor to weigh when making policy and cost choices.

Even if the idea of securing birthdates, social security numbers and payroll information seems relatively new to entertainment companies protecting intellectual property is not. Intellectual property is the stock and trade of entertainment companies. By and large these companies are in business because they exploit original works of authorship (film, television programs, music, photographs, books, articles, literary works, video games and their progeny) and to some extent patents (Sony PlayStations, earbuds, mp3 players and the related technologies enabling other entertainment gadgets). Intellectual property law protects such works so it is surprising that Sony, as a rights owner, did not protect its films. Five films, four of them unreleased, were dumped onto file-sharing sites. While it is not certain, it does seem that these films were sitting unprotected on servers. Even more surprising is that Sony, part of the parent company Sony Corporation was not more proactive in protecting its film IP.

After all Sony Corporation’s music division, Sony Music Entertainment, was so concerned about unauthorized copying of its Compact Discs (“CD’s”) that in 2005 it embodied a program on its discs that among other things prevented the copying of music. In addition to several government investigations into the software and its purposes, the backlash from consumers and hackers was huge. This made Sony a target for hackers. If the music division went to such lengths to protect its IP rights in the content of those CDs, it is difficult to understand why SPE did not take reasonable precautions to protect its films.

The music division was not the only part of Sony Corporation which zealously protected its IP. In 2011, Sony PlayStation, part of Sony Computer Entertainment, chose to sue several hackers who managed to jailbreak the Sony PlayStation console enabling it to play pirated games and free software and posted “how to” instructions online. The prosecution of the jailbreakers was given as the reason hackers then broke into the Sony PlayStation network exposing consumer personal information including credit card information for ten million customers. That attack caused Sony PlayStation shut down its network for 24 days and cost the company $171 million. The head of Sony PlayStation called it an unprecedented attack despite the company’s strong security.[9]

**However, not everyone agreed with that assessment.**

“Outside experts…. concluded that shoddy IT practices, including a failure to install software security updates, left Sony wide open. British regulators later fined the company the equivalent of $396,100 for failing to protect private information, saying the breach “could have been prevented” and calling Sony’s security measures “simply not good enough.” [10]

Suing individual consumers and locking up digital assets intended for purchasers is not necessarily the most effective way to protect a company’s IP. Encryption, segregated placement on a server and other security measures can be implemented so that additional steps and effort are required to get to valuable information.

Privacy and cyber-security measures also serve to protect a company's intellectual property assets. If for no other reason than economic self-interest, entertainment companies should prioritize privacy and cyber-security. Lack of security or purportedly lax security on its servers is one of the surprises of the Sony hack. Individual's personal data is not a form of intellectual property, but it is a valuable asset. Personal data is collected, analyzed, aggregated, sold, purchased and analyzed again. The market and developing laws will determine the ultimate owner of such data in the United States and perhaps how it may be monetized. In the interim, all companies who collect, buy, store and analyze personal data may want to consider protecting it as the asset that it is. Protecting personal data with technological, administrative and physical measures is particularly important for the companies to whom individuals have entrusted their information through direct relationships; employers, e-merchants, online subscription services and other companies who consumers permit to conveniently store their user preferences for future reference and tailored experiences.

**Costs**

The hack has reportedly cost Sony somewhere in the neighborhood of $41-42 million dollars.[11] The exact items covered in that number are not clear. However, reports early in 2015 indicated that $35 million dollars was essentially the cost to restore Sony’s financial and IT systems. Among the other costs Sony has incurred and presumably continues to pay for: litigation from current and former employees, investigate the root cause of the hack, officially notify individuals whose personal information was breached, provide credit monitoring to the same, legal costs apart from litigation, public relations/communications strategists and the difficult to quantify cost of not operating normally for weeks and months.
Sony may have lost money overall on “The Interview” (the film at the heart of the hack), however, it has been the biggest Video On Demand release to date.

**Co-Chairperson of SPE, Amy Pascal is no longer in her title role. Instead, she has a production label with Sony.**

The employees whose information was compromised may be compensated financially, depending on the outcome of the lawsuit(s) and whether they joined the class actions or not. The emotional costs to those individuals however are not as easily quantified.

**Lessons**

Nothing can be 100% secure. Cyber-security measures and privacy practices are not a magic bullet. However, that does not mean that precautions should not be taken. After all, we lock doors, cars, windows and bank vaults even though all of these are capable of being penetrated. Cyber-security is most effective when approached in layers. In the same way that physical locks and alarms serve as deterrents, there are measures to deter a total takedown as Sony experienced.

Below are some best practices within the privacy and cyber-security realm which if Sony had had in place may have diminished some of the impact of the 2014 hack. Either way, they are practices your clients should definitely consider.

**Lesson # 1**

Email Retention policy. The most publicly discussed aspect of the Sony hack was the posting of internal emails. While we can all say in hindsight how silly it is to put certain things in an email, the fact is that people do and will continue to state things in an email that they probably should not. An email retention policy means a company regularly deletes and destroys emails after a certain period of time. This will help your client limit exposure from a breach and potentially help in litigation as discovery and exposure will be limited if deletion of emails is part of your standard operating practice. Archiving emails after a certain period and automatically deleting them from employees’ accounts as well as company email servers is a good practice under all circumstances. Regularly and systematically deleting items older than 90 days, 180 days 360 days may also help efficiencies as employees and contractors will have to act upon items in a timely manner and they will know that they cannot rely on keeping emails indefinitely for information. The exact time-frame is obviously specific to your client. However, the fewer old emails are kept, the better. Exposure is limited in the event of litigation or a breach. From a financial perspective, fewer emails also mean less storage and maintenance is required helping to bring down costs. Fewer emails to maintain will also likely make corporate IT departments happy.

Of course, there may be emails which need to be maintained for specific, well-thought out and justified purposes. In these instances, consider segregating such emails from the rest of your data storage and exchange/email server so that they are not readily accessible by anyone who may access the network. If these certain emails are that important, in addition to segregating them, encryption is another option to explore.

**Lesson # 1a**

Email Policy. Closely related to an email retention policy is a corporate email policy. Most companies have some sort of policy regarding email. These may or may not be combined with use policies that state some version of the following: "company email is intended for corporate use and purposes only, no sexual or other harassment may take place via email, all emails sent via the company system (internet connection) belong to the employer and may be read by the employer at anytime."[12] These are not new. I read something similar back in 2001, when email and internet use was still ramping up. (Most people had dial up internet access at home and many businesses still messengered or faxed documents). It was clear from that employee handbook that even checking personal email through that company’s internet connection was subjecting strictly personal email to potential corporate seizure and “ownership.”[13] I took it seriously and never checked my personal email from work. Admittedly, I am the exception who takes such admonitions seriously. Most employees do not adhere to such policies and most employers to not enforce these policies, if they have them. Enforcing email (and all) policies is the second prong of developing a policy. If a company does not enforce a policy in a predictable and equitable manner, it is as effective as not having one at all. Among the laundry list of do’s and don’ts via corporate emails, consider advising your clients to develop their own corporate email etiquette. Establishing boundaries appropriate for your clients’ environment is important. While it may seem like common sense not to disparage co-workers at all and definitely not via email, clearly stating that this is against company policy may help prevent embarrassment and unintended consequences. In the wake of the Sony hack, there are reports that some companies are reminding workers not to put anything in an email they would not want their grandmother to read or that they would not be comfortable being made public.[14] Whether clearly stated or not, the fact is that anything in company email is likely to be treated as company property and someone other than the intended recipient is very likely to read it. Help your client and its employees by clearly stating so and reminding them regularly.
Lesson # 2

Employee Training. It is important that employees are trained on company policies and procedures. That does not mean simply giving employees a handbook when they begin and expect they know the policies. As policies are updated, training should also be updated. The most effective way to educate a workforce is to provide regular reminders in different formats and platforms so that employees really know the policies, what they should and should not do and how they will be held accountable. Consequences need to be a part of policies.

Cyber-security training is probably a new addition to most companies outside of the financial and healthcare industries. Employees, including the c-suite, and contractors should be trained to recognize phishing, spear-phising, and other methods fraudsters use to get into your clients’ network.

“Phishing is an e-mail fraud method in which the perpetrator sends out a legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites.”[15]

“Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by “random hackers” but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information..... the apparent source of the e-mail is likely to be an individual within the recipient’s own company and generally someone in a position of authority.”[16]

And there are other schemes. [17]

Hackers are continually updating, improving and inventing new scams. They are becoming more sophisticated. As such, employee training cannot be a one-time event. Cyber-security and privacy training needs to be ongoing, updated and provided in different ways. In addition to written policies, consider interactive educational programs, rewards for spotting scams and capitalizing on things like cyber-security awareness month (October) and day privacy day (January 28th). Your clients cannot afford to be oblivious to the most common methods of infiltrating their networks. Continual training and reminders will help ensure that all employees, contractors and others using or accessing your clients’ networks are aware and know what to do if and when they receive a potentially dubious email or phone call.

One of the most common ways that corporate information gets into unauthorized hands is by the loss of portable devices; laptops, tablets, smartphones and jump drives. Make sure your clients think through policies on the handling of these devices, ownership of the devices and their contents as well as what may or may not be put onto portable devices. As importantly, the workforce needs to be clear on who to call and when, if any of these is lost or misplaced.

Lesson # 3

Passwords. Do not keep a list of passwords labeled passwords unprotected on your network. In December 2014 the LA Times reported that “Sony employees had personal and corporate passwords in unencrypted documents on work computers.”[18] Many got a chuckle that such files existed on the Sony network. While this seems an obvious faux pas, it’s not unusual for people to do it. Check with your clients’ organization, it is likely that such files have (or do) exist.

Network administrators have corporate passwords or at least the ability to reset passwords. These individuals should know not to keep a file named “passwords.” Any electronic keys to passwords or to generate passwords should be kept securely and access to such keys and capabilities should be limited to key administrators.

Individual employees should know not to share their passwords, keep them written on their desks, monitors or other obvious places. Remind them at every opportunity. To raise even more discontent, passwords should be robust - upper & lower case, numbers and symbols and lengthy-, changed regularly - companies can require passwords to be changed every 60, 90 or 120 days or the user will be locked out and singular - users should not use the same password for everything but rather have a different password for every device, account, access. The importance of this is that infiltrating a network can be as simple as entering by guessing an employee’s user name and password by checking pet, spouse, children’s names on the person’s FaceBook account. If an all purpose password is hacked, then the hackers have access to everything – social media, bank accounts, sensitive documents and so forth. Of course, the more onerous the rules regarding passwords, the more likely users are to forget them and request password resets, to write down their passwords, and disregard other preventative measures your client has instilled or tried to instill. Explore what will work with your clients’ particular environment and the best ways to get user buy-in to a robust password policy. Your client should weigh the inconvenience and cost of a good password management protocol with the inconvenience and cost of a breach or hack.

Lesson # 4

Encryption. Encryption is a scrambling of data so that it cannot be read easily by unauthorized individuals. Webopedia defines encryption as: "the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.”[19] As an effective way to secure data, encryption should be considered for your important and sensitive data.[20] As discussed above, among an entertainment company’s greatest assets are its intellectual properties: films,
master recordings, original manuscripts, code, prints, etc. It seems incomprehensible that these company assets which cost a great sum to create, acquire, maintain and exploit would sit unprotected on a server. Encrypting the originals seems logical as does limiting the number of copies floating around on the network and other places such as employees’ phones, home computers and third party sharing services such as Google Drive, Dropbox and the like. When motion picture companies send out screening copies of their films (or provide a link for downloading) they are either encrypted, not capable of being copied, or watermarked with a code corresponding to the particular recipient. They also come chock full of copyright warnings and threats if the screening copies are used in anyway other than for viewing by the recipient.

Encryption is a tool to also consider for employee data and other confidential corporate information. Names, Social Security Numbers, Drivers’ License Numbers, Government ID’s, Salary Information and Financial Account Numbers as well as items in an employee’s record which may be related to health conditions or disciplinary actions are all items to be handled with extra care. Encryption should be considered for this data if it exists in digital form. It is best to keep this type of information on a segregated, sectioned off portion of a server with access limited to only those who need this information for their particular job function.

While not specific to the Sony case, consumer-facing companies which accept credit cards for payment need to abide by the PCI-DSS standards (Payment Card Industry Data Security Standard). The 12 basic requirements do not require encryption of data at rest (on the server) but do require encryption for transmission via the internet.[21] If your client sells directly to consumers, encryption should at the very least be on their radar. Using a third party to process credit card payments does not absolve your client; the end product or service provider is responsible for third parties involved in the flow or processing of credit and debit cards.

Lesson #5

Updates and Patches. This seems like one of those “no brainers.” Of course your clients’ IT department should update firewalls, anti-virus protection regularly and install patches for software as soon as these are available. But, spend some time speaking with IT in order to understand some of the challenges and whether or not this is really happening and happening across the company. The bigger the company, the bigger the challenge to update regularly, timely and with minimal disruption to the business. Once again, despite the inconvenience, the failure to update patches can help wreck havoc in an organization. One of the benefits of updating software patches is that known vulnerabilities are addressed.[22]

Lesson #6

Breach/Incident Response Plan. The time that you learn of something going wrong with your client’s network or that confidential information has been exposed is not the time to figure out what to do next or who to call. A breach notice plan is not required for most industries and definitely not the entertainment industry. However, several states have laws and regulations which almost make having a written breach response plan de facto. The State of Massachusetts requires an information security program intended to protect its residents. If your client has employees located in Massachusetts or sells to consumers there, a written plan is highly recommended.[23] Massachusetts notwithstanding, a written plan is a good idea considering that notice to individuals whose personal information may have been accessed by someone without authorization is required in 47 States and 4 territories. Each of these defines personal information a little differently. Precisely what will trigger a notice, when officials need to be notified, which officials are notified and at what point in time differs. The best way to navigate this is having a written plan. Of course working with one of several companies who provide the notice for your client and guide you and the client through the process is helpful. However, you should be aware of what is required and if you or your client will use a company for breach notification, contract them before their services are needed.

In addition to which authorities to notify, when and how to notify potentially affected individuals, a key component of a breach notice plan is having a public relations company or company spokesperson at the ready. This person (or company) needs to really understand your client’s business and philosophy and be ready on very short notice to help with the communication strategy. Who will speak on behalf of the company, at what point in time and what information will be imparted are critical for your client’s reputation. Think back to the gaffes made by the CEO of BP Oil after the Deepwater Horizon explosion and spill. Another example of a CEO having to walk back or change comments was Target’s CEO after the data breach in December 2013. There is a fine line between informing the public, trying to be transparent and publicly announcing a breach too early in the process when your client does not fully understand what has been compromised and how the company will respond. An important aspect in surviving a data breach is having a general communication strategy in which a specialist helps to formulate and then tailors the message to the particular situation.

Note that many of the state breach notice requirements will not apply if the information in question has been encrypted and the key has not been compromised. This factor should also be considered in determining the cost of encrypting certain (if not all) data.
Lesson # 7

Other Practices – There are a variety of good practices that your client needs to consider in its efforts to secure as best as possible confidential, proprietary and individuals’ personal information. The size of your client will help inform how much of the following is applicable. However, no company can afford to just ignore privacy and security measures.

- **Data minimization** is the concept that you collect and maintain only as much information as you need for the purposes you collect it. Data analytics can be a great tool for marketing, improving existing products and developing new ones. And, the more data you have in your system, the greater the likelihood that something can go wrong with all of that data. The idea of “collect it all and figure out what to do with it later” is not an optimum strategy. More is not necessarily better. If you do not need certain data for a project or specific purpose, you are better off not collecting it in the first place. In addition, once you’ve completed the objective for which you obtained the data in the first place, permanently and completely delete it from the system, not just a user’s individual machine.

- Dual Authentication for access to sensitive data, for specific users or, perhaps to access the network altogether. Dual authentication means the user can only access the specific data or network with a password and another item such as a fob[24] which generates a unique number, or a password or set of numbers sent to a cell phone.
- Firewalls around the server(s) and firewalls around certain parts of the server(s) that contain confidential, sensitive or proprietary items.
- Monitor the network and logs to understand the activity on the network. One of the best ways to understand when something unusual is happening with a network is to have a good grasp of “normal” activity and usage.
- Data mapping and data flows are great to have so that the organization knows how data comes into the system, where it goes within the environment and how it leaves.
- Cyber-liability insurance should be reviewed and updated in accordance with the risk to the organization (highly sensitive information contained on servers) and risk tolerance.

**The Upshot**

The Sony hack of 2014 was crippling, costly and embarrassing. The company was definitely down for a while but, it is not out. It is not out of business, out of financing, employees or, even out of the film blamed to be the impetus for the hack. So, what is ultimately the moral of the story? It may simply be that all companies; large and small whether in entertainment or heavily regulated industries are susceptible to hacks and breaches which will make valuable information (data) available to the “wrong” people. As more and more of our personal and other information is digital and accessible via the internet and our digital footprints get bigger, we may all want to pause and take certain precautions personally as well as on behalf of our businesses.

**Bio:** Maia Spilman, CIPP[25], is an Information Privacy and Intellectual Property Attorney based in New York City. She helps clients understand the legal obligations connected to the electronic information companies collect, use and maintain. She works with clients in the pharmaceutical, technology and entertainment industries to implement appropriate safeguards for digital data. She is a seasoned transactional attorney, has headed her own practice for more than a decade and has worked as in-house counsel for a variety of companies. www.maianyc.com

**Endnotes:**

[1] “Annie,” “Mr. Turner,” “Still Alice,” and “To Write Love On Her Arms,” were not released “Fury” was already in theaters at the time of the data dump. Information from Deadline.com
[7] Identity Theft is when another person poses as you and obtains driver’s licenses, passports or social security cards with your name and date of birth. The other person can also open credit lines, buy homes, cars and other items all in your name with your vital identifiers; date of birth, social security number. This makes it so that the victim of identity theft must always prove they are who they say they are and that the other person with all the same identifiers is actually the fraud. Credit fraud is when your credit card or bank information is stolen and money is taken from your account. In most instances credit card companies will pay for the majority of loss above $50. It is an inconvenience to the consumer and a cost of doing business to banks/credit card issuers and merchants. In the long run this increases the cost of goods and services but, it does not rise to the level of identity theft which potentially follows a person around for life.
[8] The type of data needing extra care includes: social security numbers, driver’s license number or government issued identification card or document, dates of birth, financial account number along with password or code, information, medical information and medical history.
[10] ibid
[12] Sample of the type of language used only; not a direct quote from any particular company.
What after the Sony Hack? Examination of the Development of Cybersecurity Law in the United States and in France and Its Impact on Lawyers

By Zelda Gerard

Introduction. The amount of news around the Sony hack continues to be pretty intense, despite other significant breaches and disclosures coming to light.[1] Attackers targeted a wide spectrum of industries in 2014.[2]

The Sony hack is not the first big attack: there was the Symantec source code breach of 2006 (acknowledged by Symantec in 2012),[3] Innodata Isogen breach of 2012, and Russian company SearchInform in March 2014,[4] just to name a few.

On November 21, 2014, a cyber extortion attempt was made against Sony Pictures Entertainment (SPE) CEO Michael Lynton. On November 24, SPE discovered that it had lost control of its systems. On December 19, 2014, President Obama officially laid responsibility for the attack on the government of North Korea.[5]

The devastating Sony hack seems to be one of the most mediatized hacking in the history of cybersecurity. It did trigger the resignation of Sony’s vice president on account of racist statements. It is also said that Sony’s financial loss may amount to $35 million dollars.

As another consequence of the hack, a motion was filed by former and current employees of Sony Pictures Entertainment. The notice of motion is dated February 9, 2015 before the United States District Court Central District of California – Michael Corona and Christina Mathis v. Sony Pictures Entertainment. The motion indicates that “All of these cases have been filed generally on behalf of the proposed class of former and current employees of Sony Pictures Entertainment Inc. (“SPE”) and other persons whose personal information and/or medical information is “alleged to have been compromised as a result of SPE’s data breach publicized in November 2014.”

The Sony attack is now a well-known fact, largely commented upon. The events can be briefly summarized as follows: It is said that a team of hackers gained access to Sony Pictures Entertainment Culver City network in late 2014 by sending spear phishing emails to Sony employees. Those emails contained an attached .pdf document that was loaded with a Remote Access Trojan (RAT). Once Sony employees’ computers were infected, the hackers used advanced pivoting techniques to gain access to the Sony Pictures Entertainment network in Culver City, CA.

Theories have since been developed, either tending to show that Korea was not involved, or at least not its government, but that Russian hackers also breached Sony and obtained access to Sony’s network.[6]

THE THREAT

In an order issued by President Barack Obama in February 2013, the President expressed that “the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges.”[7]

Indeed, the threat landscape is continuously changing and security incidents can endanger user confidence. While severe disruptions of electronic communications, infrastructure and services can have a major economic and social impact, everyday security breaches, problems and nuisances also risk eroding public confidence in technology, networks and services. [8]
2014 was even called “the year of data breach.”[9]

A basic definition of cybersecurity as treated under U.S. law is “whether and how electronic data and systems are protected from attack, loss, or other compromise.”[10] What exactly is at risk in the event of a cyber attack? The consequences are mostly financial losses, but not only and it is reported by PriceWaterhouseCoopers that in 2012, about 38 percent of businesses experienced financial losses but also suffered intellectual property theft and brand of reputation damage as part of the consequences of the attack.[11] Potential damage to reputation is one of the most if not the most feared consequence of cyber attack,[12] and in the Sony hack case, damage to reputation of the company indeed occurred.

THE ANSWERS

In the United States

The imposition of data security and security breach notification obligations on entities that own, possess, or license personal information is a recent phenomenon.[13] What is the application body of laws applicable to cybersecurity? First there is a patchwork of legal topics incorporated, such as privacy concerns, data breaches, information sharing, intellectual property, defamation, patent theft, trade secret, information sharing, multiplying the number of relevant acts and case law. Then, it appears that more than 50 federal statutes address aspects of cybersecurity in some capacity, whether directly or indirectly.[14]

It is almost impossible to list the applicable bodies of laws and regulations dealing with cybersecurity without mentioning the legal framework of the National Institute of Standards and Technology (NIST). Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life of U.S. citizens.[15]

The drafting and release of the Framework was made pursuant to an order issued by President Barack Obama in February 2013, recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure.[16] The order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.[17] In February 2014, the NIST released the Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework).[18]

The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure and better manage and reduce cybersecurity risk. It was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

In an update published by the NIST on its website on July 1, 2015, NIST stresses the fact that “since releasing the Framework in February 2014, (…) the framework is being employed across the country, in a host of sectors, and by organizations ranging from multinationals to small businesses” and that “the proposed value of Framework has been validated through a large volume and breadth of interactions between NIST and industry.”

The framework is guidance and its use is voluntary. However, the FAQ of the framework available on the NIST website highlights that its use has revealed helpful in raising awareness and communicating with stakeholders within their organization, including improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. It provides a map to current cybersecurity management approaches, and the FAQ also indicates that “some parties are using the Framework to reconcile and de-conflict internal policy with legislation, regulation, and industry best practice.”

In France

As France is part of the European Union, it is important to mention the initiatives taken in terms of cybersecurity at the European level when examining the legal framework in place in France.

Europe. The European Union Agency for Network and Information Security (ENISA) was established in 2004 for an initial period of five years by Regulation (EC) No 460/2004.[19] More than ten years later, ENISA is still in place and very active. It is a center of network and information security expertise for the EU, its member states, the private sector and Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks.

The European Commission and High Representative’s 2013 Cyber Security Strategy was the EU’s first comprehensive policy document in this area. It covers the internal market, justice and home affairs and foreign policy angles of cyberspace. France actively contributes in implementing the EU’s five strategic priorities:
• achieving cyber resilience;
• drastically reducing crime;
• developing cyberdefence policy and capabilities related to the Common Security and defense Policy (CSDP);
• develop the industrial and technological resources for cybersecurity;
• establishing a coherent international cyberspace policy for the European Union and promote core EU values.

In January 2015, ENISA published a “Threat Landscape and Good Practice Guide for Internet Infrastructure.” It details a list of good practices that aim at securing an Internet infrastructure asset from Important Specific Threats. The landscape lists five technical recommendations and four organizational recommendations, such as, for Internet Infrastructure owners and electronic communications network regulatory agencies, evaluating their current level of security by understanding the assets covered (and not covered) by existing security measures, implementing good practices procedures, building an information and communication technology security awareness and training program, etc.

France. In France, in order to better address the increasing issue represented by cyber attacks, a national agency dedicated to the security of information systems was created in July 2009, the « Agence nationale de sécurité des systèmes d’information » [JCP1] (ANSSI).

In February 2011, the ANSSI published a new cybersecurity Strategy for France and a new one shall be published in the course of 2015. As part of the reinforcement of the capacities of the government in terms of cyberdefense, a specific position was created. The appointed individual is the primary representative and point of contact in the event a cyber attack occurs.

A new “Cyber Defense” Pact has also been drafted in February 2014 to set the ambitions and proposals of the Ministry of Defense up until 2019.

It should also be noted that companies may be tempted to hide such attacks have been committed. The first trend highlighted by Mandiant in their 2015 report, is “struggling with disclosure” The report explains that “providing factual information based on an understanding of the scope and extent of the compromise can help organizations craft a clear and confident message when they disclose a security incident. By doing so, they may avoid having to correct and qualify past statements—and losing credibility in the process.”[20]

Economic issues are also at stake. “Regardless of whether an organization is making a public disclosure or not, it is important to understand that while key stakeholders always want answers right away.”[21] We can see that the issue of public disclosure and information of employees and customers is an important one both in France and in the United States.

In Brussel on 28 January 2015, a press release was published on the occasion of the 9th European Data Protection Day. The European Commission proposals for a comprehensive reform of the EU's 1995 data protection Directive aim to strengthen privacy rights and boost Europe's digital economy. Among these proposals was the “right to know when your data has been hacked.” For example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures.[22]

CYBERSECURITY AND LAWYERS

The emergence of cyber law

Cyberlaw is a growing field of legal practice and the roles that lawyers play in helping companies respond to cybersecurity threats.[23] Indeed, lawyers must play a role in designing the procedures, training, and risk assessments required to implement managerial, operational, and technical controls needed to protect data.[24] Very recently, companies involved lawyers mostly in the response to cybersecurity incidents rather than proactively, and this situation is apparently changing and moving towards a further involvement of lawyers preventively.[25]

This is important as recent studies show the increase in the need for lawyers specialized in cybersecurity. Why can lawyers be particularly efficient in treating cybersecurity issues? One answer can be found in the fact that as many elements covered by the term cybersecurity involve management of data, and that IT staff may not be aware of the regulatory and legal requirements associated with such data. A recent study conducted by Hanover Research[26] show that it is becoming increasingly common for companies to involve legal counsels in cybersecurity matters, either by seeking legal assistance from law firms, or hiring specialized in house counsels, and this both in the United States and in France. Unfortunately though, the study also shows that companies are more likely to involve lawyers as reactive measures, after an incident has already occurred.[27]

The continuing evolution of the legal framework for cyber security should only increase the role of lawyers in addressing these concerns,[28] both preventively as well as part of the handling of incidents and crisis.

Professional aspects for law firms – the ethics of data breaches

What are lawyers’ responsibilities in terms of protecting their clients’ data? A recent ABA commission on Ethics noted that lawyers have a responsibility to stay informed of technology development and risks.[29] It is clearly stated that
“the objectives of the ABA Commission on Ethics 20/20 has been to develop guidance for lawyers regarding their ethical obligations to protect this information when using technology, and to update the Model Rules of Professional Conduct to reflect the realities of a digital age.”

As part of this effort, the Commission asked the ABA Center for Professional Responsibility to work with relevant entities within the Association to create a centralized website with continuously updated and detailed information about confidentiality-related ethics issues arising from lawyers’ use of technology, including information about the latest data security standards.

If raising awareness among lawyers is indeed one of the ABA’s priorities, bringing lawyers to change their habits and those of their clerks or paralegals can be a little more difficult. The difference between lawyers implementing new measures in order to reinforce the security of the information they are entrusted with often depends on whether they were already themselves victims of an attack or not. “There are two types of firms: those that know they’ve been attacked and those that don’t,” said Jill D. Rhodes, co-author of “The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals.”[30]

Why is this topic important and why are law firms at risk?

The setting up of protective measures against incidents of data breaches is paramount to almost all companies and business, in many different areas, as virtually every business collects and stores personal information on both employees and clients. But, as pointed in an article by Scott Ferguson, “law firms generally have greater volumes of sensitive data in their computers and file cabinets, making the protection of that data critical to maintaining the trust and privacy of their clients.”[31]

The most commonly reported cyber breach experienced by law firms is that related to the loss or theft of a laptop, thumb drive, smart phone, tablet or other mobile device.[32] It is also considered that “experts believe that law firms are the perfect potential target given their relative lack of data security combined with a likely treasure trove of valuable information - including valuable client confidentialities and personally identifiable information.”[33]

What are the legal consequences for a law firm in the event of a data breach incident?

Besides the common law duty owed by attorneys to protect the confidential information entrusted to them by clients, two additional sources of duties are imposed on attorneys to protect data: the Rules of Professional Conduct, and federal and state law.[34]

All 50 states have an ethical rule that provides that a lawyer shall not “reveal information related to the representation of a client unless the client gives informed consent,” subject to certain exceptions including preventing a criminal act and preventing the client from committing a fraud. (see Rule 1.6 on Confidentiality of Information, which governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client).[35]

The comment given by the ABA to this rule includes the following explanation: “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

The Comment references Model Rule 5.1 (Responsibilities of a Partner or Supervisory Lawyer) and Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistant), which are also important in attorneys’ use of technology. Partners and supervising attorneys are required to take reasonable actions to ensure that those under their supervision comply with these requirements.

Model Rule 1.4. Communications, also applies to attorneys’ use of technology. It requires appropriate communications with clients “about the means by which the client's objectives are to be accomplished,” including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining “informed consent.” It requires notice to a client of compromise of confidential information relating to the client.[36]

Below are two examples of opinions rendered in connection with privileged information, one in California and another one in Florida.

In 2010, the Standing Committee on Professional Responsibility and Conduct in California issued an opinion[37] addressing the issue of whether an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties.[38] Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Attorneys are faced with an ongoing responsibility of evaluating the level of security of the technology they use. The use of laptop as such is not problematic.
In Florida, the Florida Bar Ethics committee issued an opinion in 2010 as well. The opinion examined the situation of lawyers using devices that contain “storage media i.e. any media that stores digital representations of documents such as printers, copiers, scanners and fax machines” have an affirmative obligation to take reasonable steps to ensure that client confidentiality is maintained and the device is sanitized before disposition.

Essentially, a loss or compromise of client data may expose a law firm to three types of claims. The first is a claim for damages where the client or a third party may bring an action to cover the costs associated with the damage cause by the breach. The second is compliance costs. According to Symantec’s 2013 Cost of a Data Breach study, the average cost to a business of each compromised record is $159. And last but not least, the reputation damage can be extremely painful for law firms which depend on absolute trust from their clients and which can be extremely harmed by any event challenging their professionalism.

The reasonable steps that a lawyer must take to ensure confidentiality include: (1) identification of potential threats and development of policies to address the threats; (2) inventorying all devices that contain hard drives that store media; (3) supervising non-lawyers; and (4) “sanitization of any device by requiring meaningful assurances from vendor confirming sanitization.”

Practical examples of risks include:
- sending attorney-client-privileged information over a public WiFi network, at Starbucks for instance;
- allowing BYOD: “bring your own device” by members of the firm without proper guidance;
- sending information over the Internet without using encryption techniques;
- taking a laptop containing privileged information home and then leaving it in a car/train etc… or having the laptop stolen during the commute;
- not locking one’s session after using a laptop or even when walking away from it during a break or interruption.

Practical examples of good practices include:
- employing encryption to protect data in storage on computers, smartphones, etc;
- designate a chief information officer to oversee the adequacy of firm policies and practices;
- implementing dedicated sessions to increase employees’ awareness and training including in respect of security and data issues;
- implementing a BYOD specific policy to control and manage the use of personal mobile devices in connection with confidential information;
- requiring members of the firm to regularly change their password;
- securing any file room;
- using anti-virus software, malware protection, firewalls, etc.;
- minimizing production of personal information, using anonymization techniques as much as possible;
- understanding security includes the storage and transmission of data through cloud computing solutions (Google Drive, Dropbox, etc.);
- establishing a policy regarding the treatment of personal information when production is unavoidable (for instance, defining rules as to conservation and destruction of such documents).

Finally, lawyers should keep in mind that clients and others whose information they may have could live in other states, and that other state laws may apply. A complete rundown of federal laws with data privacy provisions will not be attempted here, but a few of the ones most likely to affect lawyers are noted below. The Fair Credit Reporting Act restricts the disclosure and use of credit reports. The Health Information Portability and Accountability Act (HIPAA) restrict access to and use of health care information. The Employee Retirement and Income Security Act include privacy provisions applicable to employee health and benefit plans. These laws can include civil and criminal penalties.

CONCLUSION

What really happened at Sony Entertainment Pictures may never be publicly disclosed, and expressed theories will maybe never confirmed or infirmed. However, what is key is that the protection of data and the notion of cyber security extends beyond borders and involves more than one country.

Both in the United States and in France, the attacks are developing and in parallel cybersecurity law is emerging. One can wonder whether offering protection on a national level may be sufficient, as the threat may come from elsewhere, even from the other end of the world. Therefore, organizational and international initiatives are welcome, as they may help creating a uniform body of laws for several states or government.

We could even argue that cooperation agreements could help fighting international and cross border cyber attacks, or hacks created using proxies located abroad. What about creating a common warning and notification protocol applicable in the event a security breach or a potential threat is identified? It should be noted however, that the main obstacle to any notification protocol might be the reluctance of companies or other legal entities to report any incident in
their information system. Once again, cyber attacks are not only a threat to data, they are also prejudicial to the victim’s reputation and are often kept secret from customers.

**Endnotes:**


[12] See, e.g., The Emergence of Cybersecurity Law, Indiana University Maurer School of Law, February 2015
[21] E.] The Emergence of Cybersecurity Law, Indiana University Maurer School of Law, February 2015 prepared for the university by Hanover Research
[22] [23] See, e.g., The Emergence of Cybersecurity Law, Indiana University Maurer School of Law, February 2015
[28] The Emergence of Cybersecurity Law, Indiana University Maurer School of Law, February 2015 prepared for the university by Hanover Research
[29] State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179
[35] The Emergence of Cybersecurity Law, Indiana University Maurer School of Law, February 2015 prepared for the university by Hanover Research
[37] State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179
A Law Student’s Perspective—Daily Fantasy Sports: Confronting the Frontier of Legal Gambling
By Preston Barclay

Scanning sports television networks even for ten minutes,[1] one cannot help but notice an arms race between two companies – DraftKings and FanDuel – promoting the possibility that any “Average Joe” can win hundreds, thousands, or even millions of dollars in a single day simply by placing an entry fee as low as $1 to select a customized fantasy roster.[2] Such daily fantasy companies will also either match deposits made by new daily fantasy players on their sites[3] or offer free entry into lucrative contests,[4] practically paying people to play fantasy sports and win cash! Not so fast.[5]

With over 41 million people playing fantasy sports[6] and significant investments from venture capital firms, sports media conglomerates, and professional sports leagues flooding the industry,[7] daily fantasy sports have become integrated in the sports viewing experience. But are they actually legal? While daily fantasy sites cling to a fantasy sports carve-out provided in the 2006 Unlawful Internet Gambling Enforcement Act (“UIGEA”), should daily fantasy contests actually qualify as gambling activities that should be regulated or outlawed? Are daily fantasy games primarily based on skill or chance? Allegations that daily fantasy employees playing on other sites may have access to information unavailable to other daily fantasy sports participants[8] have accelerated state,[9] Congressional,[10] and other federal bureau investigations[11] with the issue of daily fantasy legality even arising in the Presidential campaign process.[12]

The days of uninhibited growth and the lack of governmental intervention and regulation are over. So what should daily fantasy companies do to survive and prosper? This article explores the birth and explosion of the daily fantasy sports industry, federal and state gambling law restraints and other legal issues, and provides recommendations for how daily fantasy companies and shareholders should confront a rapidly changing legal landscape. Specifically, daily fantasy companies should frame their contests as participatory tournaments requiring “entry fees” instead of “bets” or “wagers,” avoid soliciting participants in states that classify daily fantasy sports as gambling, refrain from offering NCAA-based contests under the guise of “fantasy sports” to fall within the scope of the statute’s carve-out.[23] FanDuel, one of the industry’s “Big Two” along with DraftKings (founded in 2012[24]),[25] entered the market in 2009[26] after founder Nigel Eccles recognized that UIGEA failed to define a minimum requirement for the duration of a fantasy sports contest.[27]

**Origins of Fantasy Sports**

While traditional sports gambling provides individuals a means (albeit a largely illegal one) to predict the future outcome of player performances by wagering on particular games and specific player statistics, fantasy sports enable participants to form fictional leagues to “draft” and assemble rosters of professional athletes as if the participant functioned as an executive of a professional sports franchise.[13] Based on the players’ real-life results in predetermined statistical categories (such as homeruns or batting average), the team that performs the best in those categories over the course of the season emerges as the champion.[14] The “Rotisserie League,” the first fantasy baseball league to gain public notoriety in 1980, featured ten participants drafting in an auction style format with $260 to bid on the exclusive rights to the statistics of Major League Baseball players in eight distinct categories (four hitting – runs scored, runs batted in, home runs, and steals, and four pitching – earned run average, wins, saves and strikeouts).[15] Other leagues have since incorporated additional or different statistical categories, a “draft” style format to originally select players instead of an auction, different scoring systems (including head-to-head style weekly matchups), and of course, adaptations to other sports, most notably football.[16] Like other industries, the Internet served as a catalyst for the proliferation of fantasy sports, allowing individuals to compete against others from around the world with “instantaneously downloadable statistics” and third parties collecting league entry fees and presenting cash payouts to league winners.[17]

In addition to fantasy sports, however, the Internet also led to the promulgation of U.S. residents participating in illegal online sports gambling and poker games fostered by offshore sites.[18] To supplement federal and state laws restricting sports wagering and gambling, President George W. Bush signed into law the Unlawful Internet Gambling Enforcement Act (“UIGEA”) on October 13, 2006 holding “payment processors liable for the funding of unlawful gambling websites that conducted business with U.S. customers.”[19] As a result, online sports gambling and poker websites either left the U.S. marketplace voluntarily or were prosecuted under federal and state laws, while payment processors who continued to enable such illegal activity were also prosecuted.[20]

**The Birth and Proliferation of “Daily Fantasy Sports”**

While UIGEA thwarted online sports wagering and other forms of gambling, the statute provided a carve-out for fantasy sports to evade its definition of a “bet” or “wager.”[21] Seeking to fill the void in the market for instant gratification wagering, risk-engaging startups, led by Fantasy Day Sports Corp. in 2007.[22] entered the market providing daily sports contests under the guise of “fantasy sports” to fall within the scope of the statute’s carve-out.[23] FanDuel, one of the industry’s “Big Two” along with DraftKings (founded in 2012[24]),[25] entered the market in 2009[26] after founder Nigel Eccles recognized that UIGEA failed to define a minimum requirement for the duration of a fantasy sports contest.[27]
As a derivative of traditional fantasy sports, daily fantasy sports retain elements akin to its predecessor with participants relying on the individual performances of professional athletes generally comprising a team competing against other teams constructed by other contestants. Although a variety of daily fantasy sports models exist, the most popular forms on DraftKings and FanDuel incorporate “salary cap” restraints for selecting athletes, with players assigned particular dollar values determined by the athlete’s perceived level of skill (i.e., better players cost more to add to one’s roster).[28] Other daily models, however, depart from the traditional system by allowing players to “compete directly against the host site, rather than against other contestants,”[29] construct lineups as small as three or fewer players,[30] or bet on specific “event-based” outcomes, abandoning the lineup model altogether.[31] As its moniker suggests, daily fantasy sports contests can start and conclude in just a single day, as opposed to traditional season-long fantasy leagues that last several months. Thus, the time period from the placement of an “entry fee” to payouts to winners has shrunk dramatically, as well as the number of sporting events that ultimately decide contest results.

Seeking to capitalize on a fantasy sports market featuring over 41 million users[32] and exploding growth particularly in the daily space,[33] DraftKings and FanDuel have emerged as the primary beneficiaries of significant venture capital investments, with private funding as of October 2015 exceeding $426 million and $363 million, respectively, including $575 million combined in July 2015 rounds of funding.[34] While the “Big Two” still maintains a duopoly with approximately 95% of the market,[35] “season-long fantasy giant” Yahoo! Sports has also jumped into the daily space emerging as a third significant player in the industry.[36]

In addition to investments from venture capital firms and media conglomerates such as Fox[37] and NBC,[38] professional sports leagues and teams have also invested and partnered with daily fantasy sites[39] to capitalize on increased sports content consumption as a result of fantasy sports participation.[40] In 2013, Major League Baseball (MLB) purchased an undisclosed stake in DraftKings, while the National Basketball Association (NBA) gained a 2.5 percent ownership stake in FanDuel in 2014.[41] Also in 2014, DraftKings and the National Hockey League (NHL) entered into an exclusive multi-year sponsorship deal, while FanDuel agreed to a similar exclusive four-year deal with the NBA in addition to its previous deals with five NBA franchises.[42] FanDuel also maintains an exclusive sponsorship deal with fifteen National Football League (NFL) teams.[43] Both sites have also invested heavily in television advertising, with DraftKings and ESPN agreeing to a two-year, $250 million deal that also grants DraftKings exclusivity in daily fantasy sports content on the network beginning in 2016, as well as brand integration into ESPN’s program segments.[44] As of October 2015, the daily fantasy sports boom has engineered company valuations in excess of $1 billion for both DraftKings and FanDuel.[45]

**Daily Fantasy Liability Under Federal Law**

Discussed in the preceding section, UIGEA remains the paramount authority as the justification for the legality of daily fantasy sports based on the federal statute’s silence on a duration requirement in its carve-out enabling fantasy sports wagering.[46] In light of the commercial proliferation of fantasy sports, three other federal gambling-related statutes that predated UIGEA may also implicate the daily fantasy space.

The Interstate Wire Act of 1964 (“Wire Act”) forbids individuals and companies from engaging in the business of betting or wagering on sporting events through the use of a “wire communication facility for the transmission in interstate or foreign commerce.”[47] The Wire Act defines “wire communication facility” as any communication made through an instrumentality “used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception.”[48] Although the statute predated it, courts have held that the Internet falls within the scope of a “wire transmission.”[49]

Daily fantasy sports can avert the Wire Act’s reach by avoiding the implication that contests involve “betting” or “wagering,” or that the sites have a “skin in the game” like traditional bookies who gain when competitors lose.[50] Instead, sites need to organize their contests as participatory tournaments with an “entry fee” and a “prize pool,” while insulating daily fantasy sites from earning or losing money depending on the specific results of participants.[51] It remains unlikely that courts will outlaw contests framed this way since “countless contests engaged in every day,” such as golf tournaments or beauty pageants, would then be considered unlawful gambling.[52]

A second statute, the Illegal Gambling Business Act of 1970 (“IGBA”) authorizes criminal penalties for violations of state gambling laws, specifically relating to the financing, management, supervision, direction, or ownership of an “illegal gambling business.”[53] The IGBA characterizes an “illegal gambling business” as an operation (1) illegal under the state law in which it is conducted, that (2) involves five or more people, and (3) has been in operation for more than 30 days or has had gross revenue of $2,000 in a single day.[54]

Given that daily fantasy sites have developed into large companies, the scope of liability remains dependent on factor (1), state treatment of daily fantasy sites. Although the IGBA defines “gambling” as activities such as “pool-selling, bookmaking, … conducting lotteries … or selling chances,” it fails to limit its scope to the activities specifically mentioned in the statute.[55] Further, given that the IGBA predated the advent of daily fantasy sports, its absence in the definition fails to insulate companies from liability. If states find that daily fantasy sports (or particular models) ultimately constitute “gambling,” sites should avoid offering contests to individuals from outlawing states, such as Arizona, Iowa, Louisiana, Montana, Nevada, and Washington.[56]

Third, the Professional and Amateur Sports Protection Act (“PASPA”) passed in 1992 forbids any individual or state to operate “a lottery, sweepstakes, or other betting, gambling, or wagering scheme based directly or indirectly … on
one or more competitive games in which amateur or professional athletes participate."[57] PASPA also provides a cause of action for professional sports leagues and the National Collegiate Athletic Association (NCAA).[58]

Given the leagues’ financial ties to the industry, it remains unlikely that professional leagues will implicate daily fantasy sites.[59] The NCAA, however, may challenge daily fantasy sites given its policy against “accepting advertising from sports wagering entities,” while concluding that entry fees fall under its definition of “sports wagering” as “putting something at risk.”[60] Based on PASPA, daily fantasy sites can likely proceed with professional sports contests, but should refrain from offering games relating to the performances and results of NCAA athletes.

Lastly, UIGEA provides the latest framework for liability under federal law. While the fantasy sports carve-out offers an avenue for legality, the following criteria must be met:

“(I) All prizes and awards offered to winning participants are established and made known to the participants in advance of the game or contest and their value is not determined by the number of participants or the amount of any fees paid by those participants.

(II) All winning outcomes reflect the relative knowledge and skill of the participants and are determined predominantly by accumulated statistical results of the performance of individuals (athletes in the case of sports events) in multiple real-world sporting or other events.

(III) No winning outcome is based — (aa) on the score, point-spread, or any performance or performances of any single real-world team or any combination of such teams; or (bb) solely on any single performance of an individual athlete in any single real-world sporting or other event.”[61]

Since Congress specifically intended for the protection of traditional season-long fantasy leagues under UIGEA,[62] it remains unclear if daily fantasy sports will remain protected under federal law.[63] While factors (I) and (III) provide relatively straightforward parameters for creating legal fantasy sports contests, factor (II) requires an analysis of the amount of “skill” involved in daily fantasy games, paralleling state gambling law tests. The legality of daily fantasy contests under UIGEA predominantly hinges on this determination.

State Gambling Laws’ Effect on Daily Fantasy Sports

In addition to obeying federal statutes, daily fantasy sports companies must also comply with state gambling laws.[64] and state violations can implicate federal penalties.[65] To violate state gambling laws, most states require that a contest involves (1) consideration, (2) chance, and (3) prize.[66] Since daily fantasy sports participants deposit entry fees and winners receive cash payouts, the analysis hinges on factor (2), a state’s stance on “chance” versus “skill” in a game, similar to factor (II) in UIGEA’s fantasy sports carve-out.

States differ markedly on this issue. While a majority of states utilize a “predominant purpose” test, enabling for the legality of contests that involve more skill than chance,[67] other states analyze activities under “material element” tests that allow them to declare a contest illegal even if chance fails to dominate.[68] Further, Arizona, Arkansas, Iowa, Louisiana, and Tennessee outlaw games that involve any chance at all,[69] Hawaii uses a “gambling instinct” test, and Montana forbids any forms of online gambling.[70]

Even states that follow the same test have reached different conclusions regarding the level of skill and chance involved in fantasy sports. Although both New Jersey and Kansas follow the “predominant purpose” test, the U.S. District Court of New Jersey in Humphrey v. Viacom acknowledged the “skill involved in selecting players” as a key factor in authorizing the legality of season-long fantasy leagues,[71] while Kansas’ Racing & Gaming Commission concluded that despite the skill involved in selecting players, chance supersedes skill in all fantasy sports contests.[72]

States must weigh a daily fantasy contest’s skillful elements, specifically the “mathematical modeling and prognostication” involved in initially selecting players,[73] against elements of chance, such as “systematic” chance (e.g., “snake draft” models for selecting players that randomly allocate participant draft position),[74] “imperfect information” (e.g., potential for injury or weather cancellations),[75] and “lucky shot” chance (e.g., a golfer shooting a hole in one).[76] Proponents of daily fantasy sports distinguish it from other traditional gambling activities like horse racing based upon player selection and the multiplicity of events.[77] Dissenters, however, compare daily fantasy sports contests to poker or blackjack, activities largely outlawed despite maintaining elements of skill.[78] On the other hand, even games universally identified as “skill-based,” such as chess, involve elements of chance.[79]

Daily fantasy sports remain in a nebulous area along the skill versus chance spectrum, making state-to-state resolution difficult to project with current state gambling law tests. In October 2015, however, the Nevada Gaming Control Board notably declared daily fantasy sports as gambling, requiring companies to register for state gambling licenses,[80] essentially serving as de facto ban on daily fantasy sports in the state.[81] As a result, Nevada has joined Arizona, Iowa, Louisiana, Montana, and Washington as locales where DraftKings and FanDuel refrain from offering contests,[82] with other states are considering joining Nevada in its characterization of daily fantasy sports as gambling.[83]

Current Gambling-Related Legal Issues & Impact on the Daily Fantasy Industry[84]

Daily fantasy sports largely avoided governmental interference until September 2015 when DraftKings employee Ethan Haskell inadvertently released lineup data from DraftKings’ “Millionaire Maker” tournament the same weekend he won $350,000 in a FanDuel contest.[85] While DraftKings significantly other daily fantasy platforms,[86] Since DraftKings and FanDuel contest models largely mirror each other, the potential for access to roster information trends exposed the
possibility of "insider trading" by utilizing the trends to form algorithms to increase chances at winning contests on the other sites.[87] While an independent investigation headed by Greenberg Traurig cleared Haskell of any wrongdoing, determining that he received the data after rosters locked,[88] daily fantasy sites banned employees from playing on other sites after the scandal.[89] Nevertheless, class action lawsuits have been filed against daily fantasy sites attacking employee access to information unavailable to other players.[90]

Since the scandal, FanDuel CEO Nigel Eccles has publicly backed regulation in the industry[91] and the Fantasy Sports Trade Association announced plans to create an independent control board to self-regulate the industry.[92] While the NFL, MLB, and NBA, still back daily fantasy sites, not surprising given their business ties to daily fantasy sites,[93] the leagues’ respective commissioners, Roger Goodell, Rob Manfred, and Adam Silver, also agree that the sites should be regulated to mitigate future concerns of match-fixing.[94] Silver, notably, also believes that sports gambling should be regulated.[95]

Recommendations for Daily Fantasy Sports Companies and Stakeholders

Although UIGEA provides a fantasy sports carve-out, daily fantasy sports companies would be naïve to interpret the statute as insulating daily fantasy sites from liability simply because they include “fantasy sports” in their contest descriptions or that player selection automatically qualifies such contests as skillful competitions. States have established balancing tests evaluating the amount of skill versus chance in games, and daily fantasy companies should conduct similar inspections of each contest they offer. Not all daily fantasy contests are alike; while some daily models may implicate gambling laws, others that parallel traditional fantasy sports protected by UIGEA may be able to lawfully continue. To more effectively satisfy UIGEA and state gambling law tests, daily fantasy companies should offer contests that maximize the number of events (i.e., games) that effect competition results and only offer tournaments with roster sizes at least as large as traditional fantasy sports rosters to emphasize the skillful elements of picking players.

Further, daily fantasy sites should avoid professional league “off days” where only a few teams play on a particular night, such as Mondays and Thursdays in the MLB. The fewer the number of games or events available to select players from, the closer the contest resembles traditional gambling. For this reason, professor Marc Edelman believes DraftKings’ one-tournament fantasy golf games remain risky for DraftKings.[96] Similar contests based on NASCAR race results analogize to horse racing since winning fantasy contests, like winning bets, rely on an individual actor’s final performance in a single race. While participants select “rosters” of golfers or drivers, the final results in single competitions dictate success. Other daily fantasy sports games, while implicating player performances, involve multiple events and avoid team results from deciding contest winners.

Daily fantasy sites should also consider monitoring the number of entrants into their competitions while increasing the percentage of participants that earn cash payouts. Traditional fantasy leagues involve close competition among a limited number of participants, while larger contests analogize more closely to lotteries (or large NCAA March Madness bracket pools), especially considering their short duration. In larger tournaments with few payouts, contest winners not only must select players that perform well, but they must also select players owned by as few contestants as possible to maximize the benefit when the player succeeds.[97] While tournament success still requires skillful prognostication, winning participants also rely on other contestants not selecting the same players, a matter left to chance. Although daily fantasy contests would be less enticing with lower top prizes, companies should consider reducing the size of their competitions while providing for a greater percentage of participants to receive cash payouts in each contest to dissuade concerns that certain competitions resemble lotteries disguised as fantasy sports.

Companies should also limit the number of athletes participants may select from the same team in a contest to mitigate the potential for match-fixing. Jacob Sommer, shareholder and gaming attorney at ZwillGen PLLC, opines that fantasy sports companies should limit the number of same-team players to “less than half” of a fantasy roster.[98] By restricting roster selection in this manner, match fixers would have to pay off multiple players in multiple contests to enable for any possibility of a fruitful scheme. Limits on contest payouts would also disincentivize such conspiracies.

Professional sports leagues should likewise consider divesting their equity stakes in daily fantasy companies while the government questions their legality. Leagues have long maintained hard stances on gambling given significant match-fixing scandals in the NBA[99] and MLB[100] that compromised the integrity of competition vital to their brands. NBA Commissioner Adam Silver’s stance for regulation in both daily fantasy and gambling suggests that while the league believes fantasy sports are legal skillful games, daily fantasy nevertheless implicates nefarious activity that warrants monitoring.

Conclusion

Ultimately, Congress will likely speak on an industry that federal statutes are currently silent, and states will continue to examine their legality under current tests or issue specific declarations. Although daily fantasy sports’ future remains largely in the hands of regulators, companies should continue to proactively institute policies for regulation and limit contest offerings to only those that closely resemble traditional fantasy sports based on as many games as possible while forcing diverse roster construction. Daily fantasy’s conceptual blend between legal traditional contests and illegal gambling presents an opportunity to narrowly apply gambling laws to limit the now multi-billion-dollar industry, broadly
eliminate the fantasy sports’ UIGEA exemption, or enable for the future legalization of all sports gambling. Regardless, the old daily fantasy sports industry free from regulation will soon be history.

Bio: Preston Barclay is a student at The George Washington University Law School, Class of 2017. He is a 2014 graduate of Georgetown University, and is the Co-President, GW Law’s Entertainment and Sports Law Association (ESPLA) and an Editorial Staff Member, AIPLA Quarterly Journal.

Endnotes


[28] See generally id.
[30] Id. at 15-16.
[31] Id. at 16.
[33] See Michael J. de la Mercé, FanDuel to Announce It Has Raised $275 Million More, N.Y. Times (Jul. 14, 2015), http://www.nytimes.com/2015/07/14/business/dealbook/fanduel-to-announce-it-has-raised-275-million-more.html?_r=0 (indicating that FanDuel’s total active user base increased over 300% in the first half of 2015 from 1.1 million in 2014); see also Kilgore, supra note 6 (discussing DraftKing’s growth from 200,000 to 2 million active users over the previous year, while speculating growth approaching 5-10 million by next year).
[38] See Darren Rovell, NBA partners with FanDuel, ESPN (Nov. 12, 2014), http://espn.go.com/nba/story/_/id/11864920/nba-fanduel-reach-4-year-exclusive-daily-fantasy-deal (demonstrating that FanDuel company data indicates that “once a fan starts playing daily fantasy, his or her weekly sports TV consumption jumps from 17 ½ hours to 24 hours).
[40] [NOTES FROM ABA FORUM PANEL]
[41] Humphrey v. Viacom, Inc., 2007 WL 1797648 (D. N.J. 2007) at *7 (recognizing that courts across the country have found it “patently absurd” to hold that “the combination of an entry fee and a prize equals gambling”).
[50] [NOTES FROM ABA FORUM PANEL]
[51] Humphrey v. Viacom, Inc., 2007 WL 1797648 (D. N.J. 2007) at *7 (recognizing that courts across the country have found it “patently absurd” to hold that “the combination of an entry fee and a prize equals gambling”).
[54] Id. at 17.
[55] Id.
[61] Edelman, supra note 17, at 18.
[62] Id. at 19.
[63] Id. at 20.
[64] Id. at 19-20.
[65] Id. at 20.
[67] Id. at 18.
[68] Id. at 24.
[69] Id. at 24.
[70] Id. at 25.
[71] Id. at 25.
[72] Id. at 25.
[82] Legal Sports Report, supra note 56.
[84] Washington Redskins wide-receiver Pierre Garcon filed a class action suit against FanDuel in October 2015 that alleges that “FanDuel uses player names and likenesses without their permission to promote their business and collect huge revenues.” Given that Garcon’s suit avoids attacking the legality of the industry and instead focuses on potential intellectual property breaches, it was not included in the body of the article. See Brent Schrotenboer, Pierre Garcon Files Lawsuit against FanDuel on Behalf of NFL Players, Oct. 31, 2015, http://www.usatoday.com/story/sports/nfl/2015/10/30/pierre-garcon-lawsuit-fan-duel-player-likeness/74889324/.
[86] Id.
[87] Id.
[90] McCann, supra note 81.
[97] Redford, supra note 85.
[98] [NOTES FROM ABA FORUM PANEL]

---

**Peek into Recent Entertainment**

*By Michelle M. Wahl*

The entertainment industry and its related litigation is a continuously evolving landscape that requires attorneys practicing in the relevant fields to have an understanding of, and experience with, a multitude of practice areas. From sports and art to music and film, each facet of the entertainment industry requires in depth knowledge of contract law, copyright and trademark laws, media law, corporate law, and the like. Given the industry and practice field nuances, controversial topics, complex and at times antiquated rules, regulations and precedents, one must spend countless hours keeping abreast of entertainment law-related developments to better educate clients and properly advise them from both a transactional and litigation standpoint. Below represents a snapshot of some entertainment related legal matters “hot off the press” and a synopsis of some current industry happenings.

**A. Sports Law Updates:**

1. Eppley v. Univ. of Del., 2015 U.S. Dist. LEXIS 2893 (D. Del. Jan. 12, 2015). Plaintiff was recruited by the University of Delaware to play field hockey and was orally offered a scholarship by the field hockey coach that was to increase from 35% in Plaintiff’s first year, to 75% in Plaintiff’s second year, and 75% or more in years three and four. The University’s coach stated to Plaintiff via email that Plaintiff would be guaranteed the same or greater percentage for years three and four that she was to receive in year two. Based on the communication, Plaintiff signed an Athletic Grant-In-Aid Contract to receive a 35% scholarship for year one, as well as a National Letter of Intent that affirmed Plaintiff’s signature and nullified any agreements which would release her from the conditions stated within the National Letter of Intent. However, during year one Plaintiff’s coach retired. Given her performance during that year, the new coach informed Plaintiff that her scholarship would be reduced to 20% during her second year on the team. Following the same, Plaintiff and her father initiated suit against the University of Delaware, its board of trustees and the new field hockey coach. Defendants were
granted summary judgment and the District Court dismissed the complaint after finding no evidence of disproportionate treatment to support Plaintiffs' Title IX claim. The Court found sufficient evidence of similar treatment of male students and explained that reliance on her former coach's representation would not suffice given Plaintiff was aware of the NCAA prohibition against multi-year promises of financial aid. More importantly, Plaintiff, having signed the National Letter of Intent, rendered any prior oral or written agreements with the former coach null and void. The case stands for the proposition that written agreements with universities will be enforced by the court and that in doing so the court will typically apply the general principles of contract law.

2. In early November 2015, a New York judge overturned an arbitration award, holding that in adjudicating a multi-million dollar interleague squabble, the MLB demonstrated an utter lack of concern for fairness. The courtroom battle involved Peter Angelos of the Baltimore Orioles and Ted Lerner of the Washington Nationals and dated back to when the Nationals were relocated from Montreal in 2005 and Angelos sought to protect his home television market. At that time, the teams negotiated a deal whereby the Orioles would hold a majority partnership profit interest in Mid-Atlantic Sports Network (“MASN”) and get to telescast Nationals games from 2005 through 2011 for a discounted rate. Thereafter, MASN would be required to pay “fair market value.” The parties resorted to arbitration in hopes of having “fair market value” determined given that there were substantial differences in how the respective parties defined the term. An MLB committee was formed in June of 2014 and a decision was made that $53 million would be paid in 2012 with various increases that would take the fees to $66 million by 2016. Attempts were made to vacate the arbitration award given the Orioles estimated lost asset value of its network at $800 million. The Orioles further complained that a $25 million payment was made to the Nationals and that such amounted to nothing short of corruption and fraud in the arbitration process. Although arbitration awards are rarely vacated, Judge Lawrence Marks held that some facts of the case clearly established a lack of impartiality during the process. However, those facts did not persuade Judge Marks that the MLB commissioner failed to act fairly or that the $25 million MLB loan to the Nationals during the dispute was enough to overturn the arbitration award on their own. Here, the issue hinged on the lawyers involved in the arbitration process. Namely, Proskauer Rose represented the Nationals, but also represented the MLB in various other matters, and was concurrently representing teams who were on the panel. The Orioles and MASN expressed their concerns regarding the Nationals' choice of counsel during arbitration, but no action was taken on the part of the MLB, arbitrators, Nationals or Proskauer Rose to address those concerns. In fact, the Court noted that had reasonable steps been taken to address the same, the Court may have been compelled to uphold the arbitration award pursuant to the Federal Arbitration Act. It was that inaction that compelled Judge Marks to rule in favor of the Orioles and MASN. Of course, the main issue regarding MASN rights fees remains unresolved and where the parties go from here, is yet to be determined. See Judge Mark's Order of the Supreme Court of the State of New York, New York City: TCR Sports Broadcasting Holding, LLP v. WN Partner, LLC, et al., Index No. 652044/2014 (S.C. NY, November 4, 2015).

3. In 2014, the United States Patent and Trademark Office’s Trademark Trial and Appeal Board (“USPTO TTAB”), canceled six trademarks then owned by the Washington Redskins and further ruled that use of the name “Redskins” was disparaging to Native Americans and thus, unsuitable for trademark protection vis-à-vis applicable federal trademark exceptions for offensive and/or disparaging language. The appellate brief filed by the Redskins’ legal team in the Fourth Circuit was replete with references to other, equally racy and/or offensive trademark registrations in attempt to establish exceptions for offensive and/or disparaging language. The proposition that written agreements with universities will be enforced by the court and that in doing so the court will typically apply the general principles of contract law.

B. Intellectual Property Matters:

Choudhury opened his own studio where the “Sequence” was practiced in a 105 temperature room over the course of 90 minutes. The book’s 1979 copyright registration was followed by the work he registered in 2002 (a compilation of exercises contained in the book), using a supplementary registration form that referenced back the 1979 book. Following the 1994 introduction of Choudhury’s “Bikram Yoga Teacher Training Course”, Mark Drost and Zefea Samson completed the course in 2002 and 2005, respectively. The two went on to found Evolation Yoga, LLC, offering various styles of yoga, including “hot yoga,” similar to “Bikram’s Basic Yoga System” in terms of postures, breathing, time and heat. After learning of the same, Choudhury filed a complaint in the Central District of California in 2011, claiming that Drost, Samson and Evolation infringed his copyrighted yoga works. The District Court granted Defendants’ partial summary judgment motion as to Choudhury’s claim of copyright infringement of the “Sequence.” Choudhury then appealed the ruling as to the “Sequence.” The Ninth Circuit held in favor of Evolation, holding that the “Sequence” is simply an idea, process or system designed to improve health—an unprotectable idea ineligible for copyright protection. In support of its holding, the Court stated that Choudhury’s book intended to communicate the useful knowledge that it contained and that disallowing that knowledge to be used would monopolize the very activity that Choudhury sought to popularize. In other words, rather than “stimulating artistic creativity for the general public good,” copyright protection of the “Sequence” would prevent the public from engaging on Choudhury’s idea and building upon it. (Citing Mattel, Inv. V. MGA Entmt’i, 705 F.3d 1108, 1111 (Ninth Cir. 2013) (quoting Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975)). Based on a similar analysis, the Court also rejected Choudhury’s contention that the “Sequence” was a copyrightable compilation and/or copyrightable choreographic work. Essentially, the “Sequence” falls squarely in Section 102(b)’s exclusions from copyright protection as it qualifies as an idea, process or system to which copyright protection may in no case extend.

2. Santa Claus is Coming to Town (and home to the original author’s heirs). – In October 2015, the Second Circuit ruled in favor of the descendants of J. Fred Coots, one of the original authors of the popular 1930’s song “Santa Claus is Coming to Town” (the “song”), holding that the song will return to them in December of 2016 pursuant to the 1976 statutory regime that gave authors and their statutory heirs the right to terminate previously made grants of copyright under certain circumstances, and thereby recapture some of the value associated with the authors’ works (17 U.S.C. §§ 203, 304(c)). Baldwin v. EMI Feist Catalog, Inc., 2015 U.S. App. LEXIS 17632, 116 U.S.P.Q.2D (BNA) 1273, Copy. L. Rep. (CCH) P30, 828 (2d Cir. Oct. 8, 2015). For more than ten years, Coots’ descendants have attempted to untangle the copyright web and terminate rights held by EMI Feist Catalog, Inc. (EMI) after Coots made certain grants to EMI’s predecessors. Plaintiffs brought suit seeking a declaration that either a Notice of Termination they served on EMI in 2007 or another such Notice served in 2012, effectively terminated EMI’s rights in the song. The District Court granted EMI’s summary judgment motion, holding that EMI’s rights would subsist through the entire remaining copyright term (i.e. until 2029) pursuant to a 1951 Agreement. However, the Second Circuit Court of Appeals reversed, holding that EMI’s rights were governed by a subsequent contract executed in 1981 and that the 2007 Termination Notice would terminate the 1981 Agreement in 2016.

The facts of the case established that in 1934, Coots and Gillespie (co-author of the song) sold the song and rights to secure copyright therein, to Leo Feist, Inc. (“Feist”). Feist registered the song for federal copyright protection that same year and at that time, copyright protection was governed by the Copyright Act of 1909. Under the 1909 Act, authors were given protection for an initial twenty-eight year period on the date of publication, with a right to renew for an additional twenty-eight year “renewal term.” By virtue of the 1951 Agreement, Coots granted his renewal rights separately to Feist and Feist renewed his copyright in the song in 1961 (at which point his rights were set to expire fifty-six years later, on September 27, 1990). In 1981, Coots served on Feist’s successor, Robbins Music Corporation (“Robbins”) a termination notice naming October 23, 1990 as the termination date for the 1951 Agreement and sent a copy of the same to the Copyright Office (although apparently, it was never actually recorded). The 1981 Agreement was then executed between Robbins and Coots, reciting Coots transfer of the song’s renewal term to Feist in the 1951 Agreement, the renewal of that copyright, recitation of the renewal term provided by the 1976 Act and language providing the remainder of copyright in the song would be transferred to Robbins pursuant to Section 304 of the Copyright Act of 1976. As part of this Robbins/Coots agreement, Coots’ children received royalty installments and assigned to Robbins all of their rights and interests in the song for the extended renewal term thereof.

In 1976, the U.S. Copyright Act went through a major overhaul. Particular to this appeal, the revisions restructured works already in their renewal term by extending the renewal term to seventy-five years from the date copyright was originally secured (17 U.S.C. § 304(b)). After passage, the rights in the song granted to Feist were set to expire in 2009. The passage also provided authors and their heirs an opportunity to benefit from the extended term. Specifically, if the author had died, certain statutory heirs had the right to terminate the exclusive or non-exclusive grant of a transfer or license of the renewal copyright that had been executed prior to January 1, 1978 (17 U.S.C. § 304(c)). The revised Act also provided that authors and their heirs had the right to terminate grants executed on or after January 1, 1978 and provided the right could be exercised during a five year period beginning at the end of thirty-five years form the date of execution of the grant. However, if the grant covered the right of publication as well, the five year period began at the earlier of (1) thirty-five years from the publication or (2) forty years from execution of the grant. Id. § 203(a)(3). Terminations under either § 304(c) or § 203 could be effected notwithstanding any agreements to the contrary. Id. § 203(a)(5).
In 1998, Congress passed the Sonny Bono Copyright Term Extension Act (the “1998 Act”) that extended the renewal term to last ninety-five years from the date the copyright was originally secured (i.e. for copyrights still in their renewal term at the time the 1998 Act was passed). 17 U.S.C. § 304(b). The 1998 Act also provided for a new termination right whereby heirs could affect termination in the same general way as § 304(c), if the termination rights provided in that section had expired by such date and authors or owners had not already exercised their termination right. In 2004, Coots’ heirs served EMI (Robbins’ successor) with a termination notice, based on the belief EMI still owned rights under the 1951 Agreement. However, EMI believed the 1981 Agreement was operative. Negotiations between Coots’ heirs and EMI began in 2006. The parties agreed that in light of the 1981 agreement, EMI’s rights in the song would terminate under § 203. Thus, Coots’ heirs served and recorded the 2007 Termination Notice, which would terminate EMI’s rights in the song on December 15, 2016. The case somewhat stalled until 2009 when EMI received notice of a copyright claim in the song from Warner-Chappell Music (the copyright administrators for a Coots family venture), by virtue of the 2004 Termination Notice. EMI claimed the termination was unavailable given that Coots had already exercised his § 304(c) termination in the 1981 Agreement and as such, § 304(d) termination was unavailable to Coots’ heirs. In 2011, Coots’ heirs sued EMI in the United States District Court for the Southern District of Florida, seeking a declaration that the 2004 Termination Notice terminated EMI’s rights in the song on December 31, 2009 or alternatively, that their 2007 Termination Notice would terminate the rights on December 15, 2016. In 2012, the Coots’ heirs served and recorded their 2012 Termination Notice, citing § 203 as the source of their right to terminate the 1981 Agreement. After the action was dismissed for lack of personal jurisdiction over EMI in Florida, the Coots heirs brought suit in the Southern District of New York on December 21, 2012 and sought the same relief. The District Court granted EMI’s motion for summary judgment, holding that since the 1981 Termination Notice was never recorded, EMI retained its rights in the song under the 1951 Agreement, which was not terminable under § 203 as a it was a pre-1978 grant. The court further held that § 304(d) was unavailable as Plaintiffs had exercised their § 304(c) termination rights when they served the 1981 Notice on EMI and were provided with a bonus payment. Ultimately, the court held that EMI’s rights would survive until 2029. This Appeal then followed.

After an exhaustive analysis of U.S. copyright law, particularly as it relates to termination rights, the Court found in favor of Coots’ descendants. Namely, it held that the 1981 Agreement not only granted EMI the future interest scheduled to revert to Coots upon termination, it replaced the 1951 Agreement as the source of EMI’s existing rights in the song. Relevant language in the 1981 Agreement clearly established the parties’ intention to replace the 1951 Agreement by virtue of the 1981 Agreement. The Court noted that consistent with its ruling in DC Comics v. Pac. Pictures, Corp., 545 F. App. 678, 680 (9th Cir. 2013), that intention may be expressed or implied. Here, granting EMI the rights it already owned under the 1951 Agreement in addition to the new interest that vested in Coots upon service of the 1981 Termination Notice, the 1981 Agreement made it clear that the parties intended to replace the earlier agreement. Further, the Court held that the District Court’s reliance on extrinsic evidence was inappropriate as the 1981 Agreement clearly established the parties’ intentions. Also, there was no dispute that before the 1981 Agreement was executed, EMI owned Coots’ renewal rights under the 1951 Agreement, and that absent the 1981 Agreement (assuming Coots recording the 1981 Termination Notice), EMI’s rights would terminate in 1990. After executing the 1981 Agreement, EMI’s rights were to survive until 2009. The language of the 1951 Agreement shows that the parties chose not only to have EMI receive the future interest that vested in Coots upon service of the termination notice, but also to replace the 1951 Agreement as EMI’s source for rights in the song. Thus, Coots’ failure to record the 1981 Termination Notice is irrelevant to whether EMI owned the copyright under either the 1951 or 1981 Agreement. In other words, whether EMI owned the song’s copyright via its rights in the renewal term or by virtue of the post-termination interest conveyed back to EMI in the 1981 Agreement, EMI’s rights in the renewal term are traceable to the 1981 Agreement, either way. For purposes of deciding whether Plaintiffs termination notices pursuant to § 203 are valid, all that matters is that EMI’s rights in the renewal term are traceable to the 1981 Agreement. Given the invalidity of the 1951 Agreement, the issue became whether the 1981 Agreement would be terminated by the 2007 Termination Notice or the 2012 Termination Notice.

There was no dispute that the 1981 Agreement was executed after January 1, 1978, that Plaintiffs owned a sufficient percentage of Coots’ termination interest and that Plaintiffs’ 2007 Termination Notice met all required formalities. However, EMI argued that § 203 was not available to Plaintiffs because the 1981 Agreement was not executed by the Author (Coots), when in fact, it was. Moreover, in 1981, the Coots heirs, who also signed the Agreement, had no interest to convey. The only rights they could conceivably convey when executing the 1981 Agreement would have been termination rights they were to inherit upon Coots’ death. However, such rights cannot be contracted away. EMI further argued that the 1981 Agreement covers the right to publication and thus, the 2007 Termination Notice will not terminate the 1981 Agreement until 2021 (i.e. forty years after execution). However, publication occurs when the work is first sold or otherwise distributed to the public, and EMI certainly could not claim that the first time the song was made publicly available was in 1990 (the date EMI argued was the first public release of the song after execution of the 1981 Agreement). In sum, the Court held that the 1981 Agreement was executed by the author and did not cover the right of publication and thus, was terminable under § 203 starting on December 15, 2016 (the effective date of termination pursuant to the 2007 Termination Notice).

3.  Point Break Spoof – Innovative or Infringing?  In Keeling v. Hars, Plaintiff sought to enforce a copyright in Point Break Live, an unauthorized parody stage adaption of the 1991 Point Break movie. For the play, Plaintiff added jokes, props,
humorous theatrical devices, and exaggerated staging to transform the plot and dialogue of the Point Break movie into a theatrical experience. The Defendant, Hars, owns New Rock Theater Productions and had executed an agreement with Plaintiff in 2007 whereby New Rock would stage a two-month production run of the parody play. After the initial run, Hars attempted to renegotiate his agreement with Plaintiff pursuant to his understanding that she did not own any rights to the parody play. Plaintiff then registered the parody play for copyright protection (without first obtaining permission from the copyright holders of the original Point Break movie) and threatened to file suit against Hars. However, Hars continued to stage performances of the parody play without compensation to Plaintiff for four years thereafter. In 2010, Plaintiff brought suit against Hars, New Rock and the latter’s investor, asserting copyright infringement, breach of contract and tortious interference with contract claims. Following a series of defense motions, the District Court denied the same on the basis that a parody that makes “fair use” of another copyrighted work may contain sufficient originality to merit copyright protection itself. The case then proceeded to trial in 2012 and a verdict was returned in favor of Plaintiff, finding that her use of material from the film was fair parody, that she was the sole owner of the copyright in that parody, and that defendants had infringed that copyright. Hars then appealed the District Court’s denial of her summary judgment and the jury verdict. The parties essentially agreed that under § 107 of the 1976 Copyright Act, the Plaintiff’s parody, like other comment or criticism, constituted fair use. The Court’s primary issue on appeal was whether an unauthorized work that utilized fair use of its source material may itself be protected under copyright. In that respect, the Court affirmed the District Court judgment, holding that if the creator of an unauthorized work stays within the bounds of fair use and adds sufficient originality, she may claim protection under the Copyright Act, 17 U.S.C. § 103, for her original contributions. Keeling v. Hars, 2015 U.S. App. LEXIS 19085 (2d Cir. Oct. 30, 2015).

C. In the News – Entertainment Industry Updates:

1. Kobalt and YouTube tie the royalty knot! After acquiring AMRA in June, Kobalt has sealed the deal with YouTube as its music royalty collector for videos shown on its site. The nearly global platform provides Kobalt with the right to collect these royalties in over 100 territories worldwide. More importantly, the deal will drive greater revenues (and undoubtedly more efficiency) for the writers involved by virtue of removing other collection agencies from the equation. The relationship creates a greater transparency and ability to accurately report and pay Kobalt clients. (http://www.billboard.com/articles/business/6738564/kobalt-amra-global-deal-youtube-royalties-videos), October 26, 2015.

2. Bandcamp Revamp! – In mid-October 2015, Bandcamp, a platform used by many to generate substantial income, announced that it will change how payments are made to its artists for digital sales. Namely, the same will flow through Bandcamp, as opposed to the prior model that paid the artist’s directly. Although many artists have voiced their disappointment with this policy change, the change actually allows Bandcamp to support credit cards, offer gift cards and for customers to utilize a shopping cart to purchase from multiple artists. (http://www.billboard.com/articles/business/6738386/bandcamp-ceo-payment-policy), October 23, 2015.

3. Big Business Brand Management. - In attempt to even further expand its presence in the market, Sony Music Entertainment (“SME”) has teamed up with Artist Legacy Group to provide both artists and estate brand management for Legacy Recordings and other SME labels. The venture will provide mutually beneficial services to Legacy artists and more awareness for artists through this venture and use of Threadshop (Legacy’s in-house merchandise business) and Arcade (Legacy’s creative agencies). The New York based venture will operate under the Artist Legacy Group name and reside with Sony Music Entertainment’s Commercial Music Group. (http://www.billboard.com/articles/business/6745955/sony-music-artist-legacy-group-recordings-joint-venture), October 29, 2015.

4. TVEyes Hit with Permanent Injunction in Copyright Lawsuit. Used by ABC, Bloomberg, the White House and other prominent groups and individuals, TVEyes provides its customers with the ability to download unlimited video clips and to share them with others, as well as watch live streams and prior televisions shows for a flat fee. The service caters to many well-known journalists, politicians and corporations, and provides the ability to track what cable news is saying about a particular topic. However, Fox News filed a lawsuit claiming its investment in reporting the news was being damaged by the services TVEyes was rendering to its customers. In September 2014, Judge Alvin Hellerstein ruled that indexing and excerpting programming initially featured on Fox News fell under the umbrella of fair use exception. However in his opinion, Judge Hellerstein was indiscriminate regarding TVEyes’ users’ ability to share the content. The most recent opinion, now provides that the following TVEyes activities are disallowed: (1) enabling users to download clips of original Fox News Channel or Fox Business Network content to their personal computers; (2) enabling users to view FNC or FBN content by searching date, time and channel; enabling users to share video clips of FNC or FBN content on social media websites (rather than by personally directed emails), with even further limitations. As to the latter, emailing a clip is permitted only when a TVEyes clients send it to five or fewer recipients and both the sender and recipient(s) must register their work email with TVEyes. The Judge also required TVEyes to “implement a blocking feature preventing links to FNC or FBN clips stored on any servers owned or leased by TVEyes from playing when they are accessed from links posted to major social sharing services on the internet” (i.e. Twitter, Facebook, LinkedIn,
A Law Student’s Perspective The Inside Scoop from Inside Sports:
The Business of Being Team Counsel

By Lauren Nevidomsky

Growing up, being a sports fan was second nature in my family. If you have ever met any of us, though, you know that actually playing those sports was the exact opposite of second nature for every one of us. As a result, what we lacked in athleticism, we made up in passion for our New York-based sports teams. It seems like yesterday that I was watching Wayne Gretzky’s last game and thinking this was it: hockey is what I am going to do with my life. Then, however, I remembered that I would probably get a concussion as soon as I stepped onto the ice, so I started thinking of alternative careers paths to the hockey world—one that would never require me to lace up a pair of skates.

Fast-forward sixteen years and here I am—a second year law student at the University of Virginia School of Law. I spent my undergraduate years at Binghamton University informing everyone that I would be the first female general manager of a hockey team, interning for Binghamton’s Athletic Department, and writing for BusinessofCollegeSports.com under the tutelage of Kristi Dosh. As such, when I was given the opportunity to attend the ABA Forum on the Entertainment and Sports Industries as a Student Reporter, I was beyond ecstatic. Getting the opportunity to travel to Washington, D.C., and learn from the best and brightest in the sports law industry had me as excited as a TMZ-lover getting the opportunity to hang out with Kim Kardashian for the day.[1] The Forum was a great networking and educational experience and I planned to make the most of it!

The one panel that truly stuck out to me was one titled “Inside Sports: The Business of Being Team Counsel.” It was described as an opportunity to learn about how a team’s counsel works with the different business groups within a sports franchise. Having enrolled in law school motivated partially by the dream of becoming general counsel for a major sports franchise (in addition to all the fun hours I would get to spend in the law library reading the Third Restatement of Torts), I was eager to hear about the everyday life of a general counsel, which obviously included hanging out with athletes and sitting courtside/center ice/center field for every game. Accordingly, on the last day of the conference, I filed into the room at the Grand Hyatt Downtown and sat at attention to hear from the counsels of teams in the National Hockey League, Major League Baseball, and the National Football League.

The panel included Danna Haydar, Associate General Counsel, Tampa Bay Lightning, Amalie Arena and Tampa Bay Storm; Damon Jones, Senior Vice President & General Counsel, Washington Nationals; and Robert Forbes, Assistant General Counsel, Washington Redskins. The moderator was Casey Schwab, Manager, Media Administration & Development, National Football League. All four of them provided insights into their career paths and gave us a glimpse into the “glamorous” lives of being team counsel. This article will detail two of the major themes discussed in the ninety-minute session: the career path to becoming a team counsel and the trials and tribulations of being one.

5. Big Pimpin (will not be spending Gs defending this lawsuit!) – Judge Christina Snyder held that Baligh Hamdi, an Egyptian composer who alleged that Jay Z sampled his uncle’s song “Khosara Khosara” in Jay Z’s “Big Pimpin” hook, lacked standing to pursue his claims against both Jay Z and producer Tim “Timbaland” Mosley. Hamdi attempted to apply Egyptian moral rights concepts to an American license for the song. However, Plaintiff had previously assigned all of his rights to “Khosara Khosara” to Sout El Phan, a Middle Eastern record label and thus had no standing to pursue his suit against Jay Z and Timberland. Judge Snyder reached that conclusion after hearing testimony from Egyptian law experts. Her ruling made the issue of whether “Big Pimpin” infringed “Khosara Khosara” unnecessary. (http://www.billboard.com/articles/news/6737484/jay-z-wins-big-pimpin-trial-sample, October 21, 2015)

6. Straight Outta Compton (and into Jerry Heller’s pocket?) - Jerry Heller, N.W.A.’s former Manager filed a $110 million lawsuit against numerous defendants, including NBC Universal, Legendary Pictures, Comptown Records and others affiliated with the movie “Straight Outta Compton” for alleged defamation, trade libel, false light, misappropriation of likeness, intentional and negligent interference with a prospective economic advantage, breach of an alleged 1999 settlement agreement and implied covenant of good faith and fair dealing between Heller and parties affiliated with Eazy E (for making disparaging comments), breach of oral contracts, conversion, and copyright infringement arising from his collaboration with various parties to develop screenplays that Heller claims were the basis for the “Straight Outta Compton” movie. The complaint states the film may become the largest globally grossing music-story based film ever and that damages to Heller will undoubtedly increase, the larger the success of the film. http://www.hollywoodreporter.com/thr-esq/straight-outta-compton-hit-defamation-835751, October 30, 2015.

Bio: Michelle M. Wahl is an Associate with Swanson, Martin & Bell, LLP
Shockingly, there is no one path to becoming a team counsel, or even a “suggested” one. Two of the panelists, Danna Haydar and Damon Jones, actually took time off in the middle of their law school careers to work within the industry to get the sports business acumen and connections necessary to get them to where they are today. Danna even spent her first summer after law school interning outside the realm of law in sports sponsorship. The fact that both Danna and Damon were willing to pursue sports work, either in law or another discipline, and were willing to prolong their law school careers, shows how passionate and eager they were as students to get into the sports law world.

Taking that leap of faith to take a year of absence or intern in “just” sports, as opposed to in some legal capacity, is not something most students would do. This is especially true for students who may have to pay back a massive loan debt. I am sure that if I even thought about doing something similar, the Career Services Office at UVA would do everything in its power to persuade me out of such a career choice. However, students that exemplify the choices Danna and Damon made early on are exactly what the sports world needs—individuals who care passionately about the inner workings of the industry and are willing to do whatever it takes, even if it means forgoing a coveted and well-paid firm associateship. In fact, the moderator Casey Schwab took his job with the NFL, which he acquired through connections made while at the USC Gould School of Law, after he had already planned to start as an associate at a Chicago law firm and had signed up for the Illinois bar exam. This shows that if you really want a job in sports and one that could eventually lead you to becoming a general counsel, it is sometimes necessary to take an “untraditional” path in law school and upon graduation.

That being said, taking an associateship and practicing at a law firm upon graduation does not preclude one from becoming a team counsel in any way. Panelist Robert Forbes started his legal career at the law firm of Proskauer Rose LLP. Robert was a paralegal at the National Football League Players Association for about a year before law school and then went to Proskauer after graduating the University of Virginia School of Law. He stayed at the firm until the opportunity arose with the Redskins a few years ago. Similarly, Damon Jones worked at Williams & Connolly LLP, for several years before accepting his position with the Redskins. He started at Williams & Connolly after spending time at a smaller law firm and a sports agency and clerking on the Fourth Circuit.

Now one may be thinking, “Of course those two landed sports gigs – Proskauer and Williams & Connolly are two of the premier sports mega firms.” Although that is certainly true, all of the panelists echoed the sentiment that showing business acumen, especially with regard to the league in which you are seeking a position, and being a strong interviewer are important parts of getting the job. Names like Proskauer and Williams & Connolly may help get one in the door, but if one has misspellings in their professional correspondence or is a poor communicator during the job hunt process, a candidate will be disqualified no matter how prestigious their work experience has been. One needs to make sure that he or she does not come in just espousing their love for a certain team, but rather can provide solid team support through strong analytical abilities and superb contract drafting skills. All of the aforementioned qualities can be cultivated at any law firm; therefore, gaining experience in many big law positions can be a valuable precursor to moving in-house with a sports team.

I Got the Job! What is My Day-to-Day Schedule Going to Look Like?

Once you have hustled in law school to get the requisite sports business experience, learned how to be an excellent lawyer at a law firm, and aced the interview process, you should be ready to start as counsel for a sports team…right? What most people aspiring to become counsel for sports teams do not realize, however, is how trying the life of a counsel can be at times. The function of in-house counsel for a sports team is very similar to the function of in-house counsel for any business in general—that is, to ensure that the “business” can run efficiently to generate revenue and to spot potential legal issues that may have negative repercussions on the business’s bottom-line. As an in-house legal intern for Canon Solutions America this past summer, I learned the hard way that the legal department’s resources could be stretched thin when trying to support the various business lines from pricing to sales to marketing. Similarly, the legal department in a sports team works to ensure that everyone from sponsorship to arena management to corporate partnerships are supported and in compliance with both federal and state law.

The Balancing Act

All the panelists agreed that making sure that all of the stakeholders of a team are happy while juggling requests for legal guidance from all over the organization at once is perhaps the most difficult thing to do as counsel for a sports team. At any given moment some hot issue may pop up, that may have to take precedence over everything else that the counsel was previously working on. Although some business teams may feel like their issue is getting short shrift if it is relegated, the team as a whole may not be able to function without counsel knowing how to best prioritize different legal issues and claims. On any given day, a counsel who is working on a multi-million dollar contractual agreement may be caught off guard with a litigation matter that has a short filing deadline. Yet, the very next day, a trademark issue may have to take precedence over that same litigation matter. As such, a team counsel must be extremely attentive and receptive to the changing pace and high volume of work within the legal department, as there is a little room for error if the team is going to continue being a successful franchise.
Maintaining Good Relations with the Leagues

Furthermore, one thing all three panelists discussed is the need to maintain good relationships with the respective sports leagues while attempting to create revenue for one’s team. Robert Forbes of the Washington Redskins claimed that efforts at generating revenue can brush up with some National Football League rules; despite this, his team strives to keep a good relationship with the league. Damon Jones of the Washington Nationals discussed how his team interacts with Major League Baseball on labor law issues during the off-season while the roster for the following year is finalized. Further, Danna Haydar of the Tampa Bay Lightning stated that she often corresponds with the National Hockey League on trademark issues. Recently, many of these trademark issues have to do with counterfeit and bootleg merchandising.[2] Any issue that may have consequences for a team’s league must be handled with care as to avoid possible negative repercussions for the league. Pushback from the league can make it harder for in-house counsel to do its job and may cost the team money in the long term.

Working with Contracts

Another important part of being a successful team counsel is being able to effectively negotiate and review contracts. These contracts often have little to do with the team’s players, but can span everything from vendor agreements for food sales to contracts with local car dealerships for giveaway nights. Each contract is unique in both the legal issues and stakeholders involved. For instance, in the example of a car giveaway, counsel will have to work with the sponsorship and game day logistics teams to make sure that the event runs smoothly while potentially getting regulatory approval from local, city, or state officials before the giveaway even occurs.

Additionally, many of the hundreds of contracts that in-house counsel constantly reviews deal with real estate issues. Robert Forbes said that he never anticipated dealing with regulatory issues as much as he does, as he did not anticipate the issues that inherently arise by operating practice and game day entities across multiple counties in multiple states. Each county has its own laws about how, when, and where stadiums and arenas can be built and run. Unfortunately, for the Redskins and other similarly situated teams, these different laws do not necessarily complement one another. Moreover, real estate issues often abound during renovations and upgrades to stadiums and arenas.

Conclusion

Overall, this panel was an eye-opening experience. As someone who has considered becoming in-house counsel, it was great to hear about each panelist’s day-to-day experiences. It was obvious that all three loved their jobs immensely, but their candor was nevertheless a great reminder that any job in the legal field has its stressful moments. As I begin to shape my legal career in either sports or perhaps some other practice area that I have yet to discover, I will remember this panel as a guide to not only being an effective in-house team counsel, but also to succeeding as a lawyer generally. Maybe one day I will be in their shoes as a counsel for any number of sports franchises; for now, however, I look forward to emulating what each panelist has done to keep his or her team running smoothly as a budding young lawyer starting as a summer associate in New York City law firm next year.

Endnotes


By Daphne Bugelli

As a former opera singer and future lawyer, I have always wanted to stay connected to the music industry to marry my passion for the arts with my legal education. After taking a copyright law class, I decided to focus on building a career in entertainment law. While in my third year of law school at Michigan State University, I had the opportunity to attend the ABA’s Forum on the Entertainment & Sports Industries’ Annual Meeting, thanks in large part to scholarships I
received from the MSU College of Law Alumni Association and the American Bar Association. As one of four students selected to be a Law Student Reporter, I was responsible for tweeting throughout the conference using #ESL2015. This role gave me additional opportunities to network with attorneys who were willing to share their background and advice with me.

This year’s event was held in Washington D.C. and attracted over 150 industry professionals and about a dozen law students. The conference included Continuing Legal Education panels and dedicated networking sessions where I was able to talk with lawyers involved in the sports and entertainment industries. All of the attorneys I met were very kind and willing to help students. One person I spoke with during a networking break reminded me that entertainment law is not a substantive area of the law; it is just “law with more interesting clients.” Although there are some industry-specific practice areas such as copyright litigation, he told me that working as an entertainment lawyer requires you to be competent in many substantive areas including contract law, estate planning, and intellectual property. He gave me a tip that I plan on following: “First, become a good lawyer, then start looking for industry-specific work.”

In addition to the conference’s organized networking and CLE sessions, the Annual Meeting also offered attendees the opportunity to tour some of the Capitol’s major landmarks. I attended tours of the Supreme Court of the United States and the John F. Kennedy Center for the Performing Arts along with a handful of lawyers and law students. Our SCOTUS tour was lead by a retired attorney who had argued before the Supreme Court on multiple occasions. We were very fortunate to have such a knowledgeable and enthusiastic guide. Our tour of the Kennedy Center was also excellent as we received behind-the-scenes information from the Center’s former General Counsel and the Annual Meeting’s Sponsorship Chair, Neeta Ragoowansi.

Law students were treated like any other meeting attendee and were encouraged to attend CLE workshops and panels on the topics that interested them. I attended several music-focused sessions and learned about topics such as music licensing in the digital era, the future of copyright legislation, and data security. One CLE panel that I found particularly interesting, the focus of this article, discussed the need for grand performance rights in order to use pre-existing popular music in new musical theatre performances.

A Distinguished Panel

Danielle Agguire, General Counsel and Senior Vice President, Business Affairs of the National Music Publishers’ Association, lead and moderated the discussion. The panel was made up of representatives from both ends of the performance rights spectrum. Richard Reiner, Senior Vice President, Business and Legal Affairs for the American Society of Composers, Authors and Publishers (ASCAP), spoke about the use of blanket licenses. IMAGEM’s Senior Vice President Business Affairs & General Counsel, Victoria Traube, stressed that best practices indicate, when in doubt, get grand performance rights. Experienced entertainment lawyer Andrew Owens gave background information on the topics of performance rights and the recent wave of musicals incorporating pre-existing popular music.

Background

Mr. Reiner began by telling the group about composer Giacomo Puccini’s role in establishing performing rights organizations (PROs) in the United States. The story goes that while having lunch in a New York restaurant with American composer, Victor Herbert, Puccini heard a live performance of one of Herbert’s arias and was outraged. According to ASCAP’s President, Paul Williams, “[Puccini] said to Victor Herbert, ‘Why are you not licensing this music? You should be paid for this music, because in Europe, we are.’”[1] Puccini brought the American system into question, comparing it to that of European countries where a composer would have received royalties for the performance. This discussion eventually led to the creation of ASCAP in 1914.

When an establishment plays music for guests or patrons in a public place, it is engaging in a public performance of a copyrighted work. Under the U.S. Copyright Act of 1976, “any establishment that plays copyrighted music is legally required to secure permission to use copyrighted music, whether in a live performance or by mechanical means. A music user can do this by securing licenses from the three performing rights organizations recognized by [the Act].”[2] Those PROs are ASCAP, BMI, and SESAC. ASCAP’s website lists some of the types of establishments requiring a license. These vary greatly, ranging from banks to yoga studios and beyond.[3] Any establishment can purchase a blanket license which would allow it to play recorded music within the PROs repertory without any additional cost or copyright liability. An ASCAP license would grant an establishment access “to over 8.5 million songs in the ASCAP repertory.”[4] A license from BMI grants public performance rights to “more than 10.5 million musical works”. [5] SESAC, the smallest of the three American PROs, does not indicate how many songs are included in its repertory, but it does claim to have an “international reach and a vast repertory that spans virtually every genre of music.”[6] By purchasing a blanket license from each of these three PROs, most establishments will be protected from liability. If the establishment holds live performances, however, a blanket license will only take it so far.

Dramatic vs. Non-Dramatic Performance

A large part of this CLE session’s discussion was focused on distinguishing between dramatic and non-dramatic performances. First, Mr. Owens highlighted the difference between the dramatic nature of a performance versus the
dramatic quality of a work itself. For example, a composition may be part of a dramitico-musical work by definition, such as an extract from an opera or a musical, but it may be performed in a non-dramatic manner that would not require anything more than a blanket license from the PRO which licenses that composition. Conversely, a work that was not part of a dramatic work, such as a song by pop artist Lady Gaga, could still be performed in a dramatic manner which would not be covered under a blanket license. "[T]here is no requirement that a composition be from a dramatic work to be subject to grand rights."[7] Because PROs can only license non-dramatic public performance rights, not grand rights, an establishment hosting live music needs to be aware of whether a performance would be considered "dramatic" under the Copyright Act.

The Common Music Licensing Terms page of ASCAP's website states, "Copyright law does not define the terms 'dramatic' or 'nondramatic.' As a result, rightsholders, music users and occasionally the federal courts must attempt to draw the line between 'dramatic' and 'nondramatic' performances. That line is often unclear and depends on the facts pertaining to a particular performance." Indeed, the line between dramatic and nondramatic performances is blurry, but courts often apply the two-part test set forth in Gershwin v. Whole Thing Company. "There are two basic tests to determine whether grand rights are required. Grand rights are required if: (1) a song is used to tell a story or (2) a song is performed with dialogue, scenery, or costumes."[8] Another way to state the first prong, as Ms. Traube put it, is "does the music advance the story?"

In analyzing this aspect of the performance, Mr. Owens suggested that one try mentally substituting the songs in a performance for any similar songs. Does the story still make sense? The panel put forth an example based on the rock opera Jesus Christ Superstar, Robert Stigwood Grp., Ltd. v. Sperber, 457 F.2d 50 (2d Cir. N.Y. 1972). Suppose that a local community theatre was putting on a revue where the performers sang ten of the original songs from Jesus Christ Superstar, in order, followed by three Christian hymns without the use of any dialogue, scenery or costumes. The theater held only a blanket ASCAP license. Was there copyright infringement? Mr. Owens's answer was, without question, yes. While the facts in this hypothetical are less egregious than in the actual case where 78 minutes of the original 87-minute score were performed, it is still clear that the music of the copyrighted work was used to advance the story. In fact, since Jesus Christ Superstar is a rock opera with no dialogue, only its songs are necessary to tell this story. The absence of scenery or costumes in this case does not satisfy prong two, but since courts rely on a disjunctive test, these elements are not necessary to qualify the performance as "dramatic." When an establishment holds a dramatic performance of a copyrighted work, a simple blanket license does not grant it the necessary rights. The establishment or venue must contact the composer or publisher directly to obtain grand performance rights.

**Grand rights for “jukebox musicals”**

Since the ABBA-based musical hit Mamma Mia!, both Broadway and Hollywood have seen a growth in jukebox musical popularity. A jukebox musical is a stage or film musical "compiling and incorporating popular music of a time period or the music of a specific artist or group."[9] Some popular examples include stage musicals Jersey Boys, Rock of Ages, Beautiful, The Carole King Musical, and the film Across the Universe. All of these shows took pre-existing music and created a story, sometimes based in reality, around the songs. In some cases, the songs were all composed by the same artist or belonged to the same publishing group. This would facilitate obtaining grand rights as they could all be contained in one agreement. However, some jukebox musicals, compile songs from a large number of artists. Rock of Ages uses songs by over twenty bands in one musical performance; each one of these composition's grand performance rights must be obtained from the copyright holder to avoid copyright infringement.

Although this can be a burdensome process, Ms. Traube emphasized the importance of licensing grand rights in such a situation. As the General Counsel for IMAGEM, representing the Rodgers & Hammerstein catalogue, Ms. Traube made it clear that publishers and composers will actively seek out copyright infringers. Does this mean that every pan-handler singing “Oh What a Beautiful Morning” or “Climb Every Mountain” on a street corner will be brought before a judge? Probably not. Ms. Traube indicated that composers and publishing groups such as IMAGEM tend to target performances that are generating significant revenue or are attracting crowds without the proper grand rights. Her expert advice on the topic: better safe than sorry! When in doubt, request the grand rights. It may be a headache in the beginning, but it is much better than paying the cost of court-ordered damages and facing an injunction after performances are underway. Both Mr. Owens and Mr. Reiner, along with his colleagues at ASCAP, share Ms. Taube’s view as indicated by the ASCAP website.

Whenever there is doubt as to whether specific performances of musical works might be considered to be dramatic or nondramatic, ASCAP encourages the music user to contact the rightsholders directly to get their view. If the rightsholders are of the view that the performances are dramatic, they will decide whether or not to license the performances directly (or at all).[10]

So while the Copyright Act may not be clear as to when a performance is “dramatic” or not, it is always best to avoid the drama. Getting the grand rights “at the very beginning, [is] a very good place to start.”[11]

**Endnotes**

Dear Forum Members:

Thank you for taking the time to read our winter issue of the Entertainment and Sports Lawyer. Brian Rosenblatt has once again curated an amazing group of articles and practice updates to keep our members on top of issues affecting our industry.

2016 is off to a great start for the forum! We have had two successful webinars and have just completed our fourth annual Video Game Conference at Hastings College of Law in San Francisco. The conference was organized by our board members Seth Steinberg and Rusty Weiss. We are also excited by the great efforts of Richard Rappaport and Henry Root to be partnering with the University of Miami for our Mid-Year International Symposium April 7-8. We look forward to partnering on this event for many years in the future and have a phenomenal two day program. The specifics are posted on the Forum’s website here.

And finally…We are also getting ready to announce the dates for our 2016 Annual Meeting, but we are thrilled to let you know that we are returning to the entertainment mecca of Las Vegas in October!

Please help spread the word about our group and upcoming events. I look forward to spending one and one time with each of you at one of these future meetings.

With great appreciation.

Your chair,

Janine Small