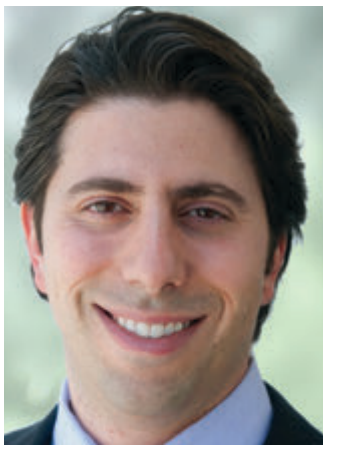
Intellectual Property & Licensing Law Roundtable

What Businesses Need to Know

As the legal landscape continues to evolve in terms of intellectual property and licensing law, the Los Angeles Business Journal once again turned to some of the leading IP attorneys and experts in the region to get their assessments regarding the current state of IP legislation, the new rules of copyright protection, licensing and technology, and the various trends that they have been observing, and in some cases, driving.

Here are a series of questions the Business Journal posed to these experts and the unique responses they provided – offering a glimpse into the state of intellectual property law in 2016 – from the perspectives of those in the trenches of our region today.



MICHAEL COHEN
Founder
Cohen IP Law Group, PC

DAN DECARLO
Partner and Co-Chair of Intellectual Property and Technology Practice
Lewis Brisbois Bisgaard & Smith LLP

JESSE SAIVAR
Partner and Chair, Intellectual Property & Technology Group
Greenberg Glusker LLP

INTELLECTUAL PROPERTY & LICENSING LAW ROUNDTABLE

'The evolution of technology and positive economic conditions over the last 4-5 years created a start-up generation of entrepreneurs. Before this change, Intellectual property used to be primarily relevant for larger experienced entities but is now being explored by the 23 year-old kid with an app idea for the next Uber, especially given the ubiquitous nature of mobile applications in everyday life. Aside from the growing changes in the law, I think the most "meaningful" change is that IP Attorneys get to a whole new set of clients.'
MICHAEL COHEN

'As with many IP attorneys, especially here in Los Angeles, I'm much more interested in how the Supreme Court will eventually rule on a case being decided right now: Varsity Brands v. Star Athletica. I have experienced the extreme frustration of clients who see their unique designs knocked off by companies who sell nearly identical pieces at a fraction of the cost. On the other hand, I know that many of the same clients are protected by the fact that certain design elements they rely upon can't be exclusively owned by one party. I'm curious if this case could lead to what I would view as a slight correction, which would prohibit blatant knockoffs but not lead to a system in which every designer is afraid of an infringement suit. That's probably wishful thinking. In the end, even if the decision does arguably expand copyright protection for clothing designs, my guess is that it would be narrowly tailored to apply to designs as unique as those for cheerleading uniforms, not pieces like evening gowns.'
JESSE SAIVAR

◆ What are some of the most meaningful recent changes to the intellectual property law landscape?

COHEN: The evolution of technology and positive economic conditions over the last 4-5 years created a start-up generation of entrepreneurs. Before this change, Intellectual property used to be primarily relevant for larger experienced entities but is now being explored by the 23 year-old kid with an app idea for the next Uber, especially given the ubiquitous nature of mobile applications in everyday life. Aside from the growing changes in the law, I think the most "meaningful" change is that IP Attorneys get to a whole new set of clients.

DECARLO: There has been an unmistakable trend to place back with the District Courts broad discretion on a number of matters that I would suspect is going to increase litigation. Most recently, in a very short and matter of fact opinion, the 9th Circuit (the Federal Appeals Court that governs the law in the western United States) joined several other circuits in making it significantly easier for prevailing parties in trademark cases and other claims based on the Lanham Act (false advertising and other claims related to conduct that confuses consumers) to recover attorneys' fees. For decades the Federal Courts in the 9th Circuit's jurisdiction were permitted to award attorneys' fees in only egregious cases where a defendant acted willfully. That standard has now been dramatically lowered- at least in the western United States- to match the standard in patent cases. The patent standard for an award for attorneys' fees was lowered in 2014 by the Supreme Court. The standard for awarding attorneys' fees in copyright cases was also lowered earlier this year. And while the Supreme Court has not weighed in on Trademark Cases, certainly when it does, it will lower the standard to match the patent standard. But even if the Supreme Court does not act, the various District Courts are already treating the question with a lower standard. The District Courts are now required to examine the "totality of the circumstances" to determine if a case is "exceptional" (which is the standard for awarding attorneys' fees in all patent cases and in many circuits now for trademark cases), which is defined simply as a case that stands out from others. That broad of a standard vests the District Courts with great leeway, which is exactly what the Supreme Court wants. To make matters even more significant for litigants, the likelihood that an appellate court will overturn a District Court on these types of decisions is similarly remote, as the Supreme Court has similarly noted that discretionary calls can only be overturned when that discretion is abused. There for, in nearly every intellectual property case, there will now be a lot more at stake, because the prospect of paying your adversaries attorneys' fees if you lose has become far more likely.

◆ Is there pending new IP legislation coming soon? If so, does this stand to help or hinder existing businesses?

COHEN: In 2016 a new federal law was passed called The Defend Trade Secrets Act. The law created a federal cause of action for misappropriation of company information, but it's not a big change, as that law existed on the state level in almost all 50 states. As congress and senate are busy filibustering each other, most of the changes to trademarks, patents, and copyrights will probably come from the Supreme and Federal Courts interpreting existing statutes. The Supreme Court is going to hear the case, "Lee v. Tam" which is known by most people as "the Washington Redskins case." The Court will decide whether or not a portion of the Lanham Act unlawfully limits the 1st Amendment. The Lanham Act currently forbids protection for any marks that "disparage persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute."

◆ What was the most surprising IP decision the Supreme Court issued last term?

SAIVAR: As with many IP attorneys, especially here in Los Angeles, I'm much more interested in how the Supreme Court will eventually rule on a case being decided right now: Varsity Brands v. Star Athletica. I have experienced the extreme frustration of clients who see their unique designs knocked off by companies who sell nearly identical pieces at a fraction of the cost. On the other hand, I know that many of the same clients are protected by the fact that certain design elements they rely upon can't be exclusively owned by one party. I'm curious if this case could lead to what I would view as a slight correction, which would prohibit blatant knockoffs but not lead to a system in which every designer is afraid of an infringement suit. That's probably wishful thinking. In the end, even if the decision does arguably expand copyright protection for clothing designs, my guess is that it would be narrowly tailored to apply to designs as unique as those for cheerleading uniforms, not pieces like evening gowns.

DECARLO: The Supreme Court's June 13, 2016, decision in Halo Electronics, Inc. v. Pulse Electronics, Inc., No. 14-1513, and Stryker Corp. v. Zimmer, Inc., No. 14-1520 was surprising. This decision changed the standard by which a patent-infringement plaintiff can recover enhanced damages. Under this new standard, enhanced damages, that is, up to three times the amount of the actual damages, can be awarded if the patentee shows, by a preponderance of the evidence, that the infringer engaged in "egregious" activity "beyond typical infringement." This standard replaces a former, rigid two-part test (an objective part and a subjective part) that previously had been formulated by the Federal Circuit Court of Appeals and used for many years. According to the Supreme Court, the rigid test excluded from punishment many of the most culpable offenders, i.e., infringers who intentionally or knowingly infringed, even though the infringement was not "objectively reckless". As a result, under the Supreme Court's current holding, it is easier for a patentee to prove that an infringer "willfully" infringed the patent, and that the court should award enhance damages. Coupled with the recent trend of attorneys' fees being more readily recoverable, the stakes in patent cases have gone up significantly as there is now a greater chance the damages will be enhanced and the losing party will have to pay attorneys' fees.

◆ What are some common copyright issues that small businesses face? How can they best be addressed?

SAIVAR: These days, many small businesses, especially those in the apparel industry, feel the pressure to regularly publish content in order to foster deeper relationships with their young consumers. Because these efforts are commonly undertaken by young people who have grown up believing that they're allowed to share anything that can be found online, this often leads to unauthorized use of copyrighted photos. With the advances in watermarking technology and the rise of law firms that specialize in finding unauthorized use of images, companies are now frequently receiving what appear to be automated demands for licensing fees. The easiest way to avoid this is for businesses to stress to their employees that online availability does not equate to permission to use. If a demand does come in, I strongly recommend that the recipient ask for proof of the rights claimed in the demand.

DECARLO: There are some high points which must be stressed to every small company including: (1) Always have contracts in place that requires creators of copyrighted works to assign the works to the small company and (2) always train your employees that just because its on the Internet does not mean you can cut and paste it for your own use. Also, every "work for hire" agreement should also have an assignment provision as a backstop in case the work at issue is not suitable as a work made for hire. Small business have to be wary that with the proliferation of the ease of reproduction of digital content, internal guidelines must be enforced and employees trained so as to prevent reproduction of content without permission from the content owner. Making sure that potential copyright infringements are properly insured is another critical area of review for small companies.

◆ We continue to hear stories about massive corporate data breaches; what exposure do local businesses face from data breaches?

COHEN: At this point we might as well assume everyone is hacked, we just don't know it yet. If a group of hackers want to breach your data, they probably will be able to do it. The best thing to do is back everything up on an external hard-drive that can't be accessed from the internet. Clouds are convenient, but vulnerable to anyone with an internet connection and a password.

DECARLO: The consequences of a data breach for a small to mid sized business can be even more catastrophic than they are for a large Fortune 500 Company. Most large companies have relatively secure data infrastructure, a cyber security incident response team, incident drills and a risk management department with experience to meet the challenge of any type of disruptive event. They also probably have some form of cyber liability insurance coverage. Data hosted by small to midsized companies is often less secure. The other preparation for a data security event that should happen to minimize its severity often does not occur in smaller companies. The result of a lower security level and little or no preparation for an event makes small to mid sized business the low hanging fruit for hackers. It is easier for hackers to get inside the firewall of small to midsized businesses. Once inside, they are less likely to be detected. This means the hacker is more likely to get access to confidential data and be able to use it for fraudulent purposes. When a business suspects it has been victimized by a hacker or malware, it will have to remediate the

situation and restore normal operations. This usually requires assistance from forensic experts. If the experts are not already on retainer, precious time can be lost negotiating the terms of the engagement. Also, the business is unlikely to get rates as favorable as those available to companies with the foresight to arrange for the services in advance. If the data was compromised, the business owner will be faced with obligations to notify state and federal authorities and affected persons about the breach. The victim of a hack may also have to involve law enforcement, if a crime was committed, as it often is. While the "crime scene" is being investigated, IT resources may be unavailable to the business. If the business accepted credit cards and that data was compromised, the company may face an investigation by the Payment Card Industry and face fines and costs to upgrade security before it can accept credit card payments again. Smaller businesses often lack the cash cushion or access to credit that larger companies have. Because of the business interruption caused by a cyber security event and the substantial costs of responding to an event, including the cost of notification, providing a call center for affected persons and providing credit monitoring a significant number of small businesses close their doors within 4 months of discovering data was compromised.

SAIVAR: In my experience, small businesses out of the spotlight are generally at low risk of being targeted by hackers. However, data breaches are one of those nuisances businesses should almost expect once they reach a certain level of success. The fact of the matter is that growing businesses rarely have the budget or sophistication to take the steps necessary to completely secure their data. Regardless, hackers are only growing in number and getting more skilled so I think breaches are only going to become more common. Businesses obviously need to take data security seriously and, the earlier they do, the better. At the end of the day, they should also have a pre-set plan in place (and a lawyer and/or consultant to call) if a data breach occurs. Scrambling to figure out a plan in the midst of a breach can put a company at risk.

◆ What are some of the most common mistakes that businesses make when it comes to intellectual property?

SAIVAR: The first is that young businesses often operate under the assumption that if they pay a third party for services, they own the resulting work product. They don't realize that a transfer of copyright ownership requires a written instrument. This is common with tech companies and I've seen this lead to sticky situations during a closing (including one situation in which a developer was able to negotiate a much better deal for itself because of the urgency of our client's situation). The second mistake I often see businesses make is assuming that if they have a properly worded privacy policy, they've satisfied their data security obligations. They need to understand that it's not the language of the privacy policy that matters, it's the accuracy. Having a picture perfect privacy policy that the company is not following is almost worse than having a deficient policy.

DECARLO: Failing to file for government enforceable exclusive rights, such as patent rights and copyrights; failing to keep good records of the people who created the rights; and failing to require employees and third-party contractors to sign written agreements that assign all of the intellectual property rights to the business. And just generally, starting a business is so challenging on the tangible side, that the very real value of perfecting and enforcing intangible rights (i.e. a company's IP) often gets overlooked.

◆ What are some aspects of non-compete agreements that businesses may not be aware of?

DECARLO: Many businesses in California do not appreciate that for the most part, non-compete agreements are not enforceable. There are limited exceptions, but California companies having employees sign non-competes as a standard practice is a bad idea. There have been employers who have taken the view that having employees sign such agreements, even if they are not enforceable, will deter competition by employees ignorant of the law. This too is a bad idea as having employees sign agreements the employer knows to be unenforceable just to chill otherwise free competition could have other negative implications.

COHEN: It is considered a policy in California that non-compete provisions are not enforceable. However, there is a very narrow exception. When a person sells the "goodwill of a business" or leaves a partnership or LLC, non-compete can be enforced in a certain geographic area. The explanation for this is that it would be "unfair" for a person to sell their business and then compete against it, which would diminish the value of the assets he or she just sold.

◆ Do the management or boards of businesses that suffer data breaches face liability from shareholders?

DECARLO: The Target breach established data security incidents as a critical concern for the boardroom and C Suite. Target's CEO and Chief Security Officer lost their jobs as a result of the breach and their handling of it. There is measurable reputational harm. Stock prices drop. Revenues are often reduced following an event. This is fodder for class action lawsuits. Over the long haul, however, the impact may be less than many fear. As the public increasingly understands data compromises are inevitable, most compromised data is not misused and steps can be taken to mitigate the impact of personal data having been stolen, the likelihood of shareholder actions is likely to decrease, assuming the company had reasonable security architectures and protocols in place. One reason the threat of shareholder action is likely to be muted is larger, publicly traded companies have the resources to withstand the shock that accompanies a reportable data breach event. Especially if the company has a robust insurance structure to defray the hard costs of a breach event, the long-term impact may be negligible. Target's stock price, for example, dipped but recovered. This does not diminish the exposure the company has

INTELLECTUAL PROPERTY & LICENSING LAW ROUNDTABLE

'Perhaps the most important thing any business can do is recognize that data compromises will occur. The question is not if, but when. Even if a Los Angeles business can avoid the problem, almost all businesses operate in an interconnected world. Supply chain partners with access to a company's data may be the cause of a breach event involving the local business's data. Data hosted in the Cloud might be compromised. That does not mean businesses are helpless. The most important thing to do is prepare. Have data security and incident response plans and budget for continuous improvement. Train employees to avoid obvious problems like phishing and ransomware attacks.'
DAN DECARLO

'The ubiquity of work-for-hire agreements has created an expectation that they should be utilized in any relationship that involves the creation of rights that may be protectable under copyright. What many businesses don't understand is that, under the Copyright Act, there are actually only nine distinct categories of works that can qualify as works-made-for-hire outside of an employment relationship. There is usually a legitimate question as to whether the rights under a software development agreement would fall under one of those categories. Worse yet, a little-known quirk in California employment law causes a contractor under a work-for-hire agreement to be classified as a "special employee" which can impose certain unemployment insurance and workers' compensation obligations on the hiring party. For these reasons, I recommend that most software development agreements should simply include assignment language instead of traditional work-for-hire language.'
JESSE SAIVAR

Continued from page 19

to regulators at the state or federal level on a variety of grounds or the prospect of actions by affected persons seeking statutory penalties based on state laws or the possibility of actions by banks or credit card issuers or action by the Payment Card Industry.

COHEN: Directors can be liable if they breach the "duty of care" or "duty of candor" owed to the shareholders. These days everyone is on notice that a data breach may occur. Failing to take reasonable security measures for your data is like leaving the front door of your house open to the neighborhood. If a director failed to take reasonable security measures or failed to disclose a data breach to shareholders, they could be found liable.

◆ What are the most important steps businesses in Los Angeles can/should take before, during and after a data breach incident?

DECARLO: Perhaps the most important thing any business can do is recognize that data compromises will occur. The question is not if, but when. Even if a Los Angeles business can avoid the problem, almost all businesses operate in an interconnected world. Supply chain partners with access to a company's data may be the cause of a breach event involving the local business's data. Data hosted in the Cloud might be compromised. That does not mean businesses are helpless. The most important thing to do is prepare. Have data security and incident response plans and budget for continuous improvement. Train employees to avoid obvious problems like phishing and ransomware attacks. Purchase cyber insurance to cover third party liability as well as business interruptions and cyber extortion. If the company does not have cyber security forensic, call center, public relations and legal resources lined up to respond to a data security event, look for an insurer that provides these resources at the inception of an event. Run tabletop exercises so the incident response team knows what to expect both in terms of what they must do and how they will interact with other team members. Audit the information system and how employees use company data regularly. When a data security event occurs, activate the incident response team, follow the incident response plan and recognize many events will not result in a reportable breach. Counsel with data breach experience should be involved from the outset. He or she provides a protective umbrella of privilege over the investigation and helps direct the response team. One of the biggest failures for Target was the ad hoc nature of the response. It undermined public and investor confidence. To make sure the event can be understood, it is critical to document what was done and why. When regulators review what happened, they will look to how well the victim adhered to the response plan. That provides a base line for future improvement. After the event concludes, time should be taken to identify the lessons learned and take steps to avoid a repeat event. Remedial steps should be identified and a plan to implement them launched. Training should be updated to instruct employees how to avoid what happened. All this should be documented because when a reportable event occurs, regulators will want to know what was done previously in response to non-reportable data security events. They will look for evidence of continuous improvement in response to data security events. A final takeaway is cyber security events are crises. Every company deals with crises from time to time. Some can be handled internally. Some require assistance from external experts. Data security incidents usually fall into the latter category. But any company has the skill set to manage crises and with the assistance of external resources and cyber insurance, any company can manage a cyber security event.

COHEN: Before a data breach, make sure your security protocols are up to the latest standards. Hire a digital security expert to audit your system, and be on-call if a data breach occurs. Afterwards, notify all parties that may be compromised so they can protect themselves from further harm.

◆ What advice would you give to an early stage technology company with respect to protecting its intellectual property assets?

SAIVAR: It goes without saying that if an early stage company has developed unique patentable technology they should speak with a patent attorney about the possibility of a registration. Unfortunately, however, most early stage companies don't yet have the money to invest in a full-blown patent application. In addition, many tech companies in LA are dealing in entertainment-based platforms or apps that likely don't include anything patentable. For companies in either situation, their best legal protection is two fold. First, they must make sure they have the proper agreements in place to own the tech they do have. Second is requiring NDAs to be signed before sharing anything of significance with a third party. Ultimately the best protection is often being first to market, as long as the product and rollout is well executed (being first to market with an inferior product, on the other hand, only invites others to improve upon the idea).

COHEN: Successful entrepreneurs never like hearing that they can't do something, but having experienced counsel on their side that clearly understands the company's technology and goals is critical. Once that trust is there, preemptive IP assessments provided by counsel can be fully followed or modified as seen fit between the client and its counsel. With that framework, analysis of the company's technology, contracts, and IP will flow into a more logical process for sustained preservation. So communicate with counsel, often, even if the issues are not readily apparent.

DECARLO: Budget for and secure enforceable, exclusive IP rights such as patents, copyrights and trade secrets as soon as possible. Conduct regular audits of the company's activities to identify protectable rights and then aggressively perfect those rights by taking the actions necessary to protect each type of right. Too often, companies sacrifice these efforts and end up paying far more later than what they saved early.

◆ Do most businesses need international protection on IP and licensing issues?

SAIVAR: I actually think many businesses over-estimate the importance of international trademark registrations. They end up spending tens of thousands of dollars on applications around the world covering marks, products or countries that end up being nearly irrelevant to the core of the business. I'd rather see them save their money to later spend on enforcement of their most important registered marks. The one exception to this is China. Regardless of a company's early interest in the Chinese market, I believe it's a good idea to seek broad registrations in China as early as possible. Without acquiring early registrations, you might as well assume that upon reaching some level of success in any other market, someone in China will register your identical mark and there won't be much you can do about it.

COHEN: It really depends on whether the business services or plans to service clients internationally or their goods reach customers internationally, then absolutely. IP covers not only copyrights, patents, and trademarks, but trade secrets as well. Even if international expansion is not in the immediate horizon, discuss and plan with counsel early because often when you snooze your lose, meaning that in many cases, such as with patents, there are statutory deadlines in which patents must be filed in foreign countries. Waiting too long to file can effectively constitute a complete bar to later file which may in turn cause a complete loss of a geographic market share.

◆ Should California companies that hire software programmers always use a "Work for Hire" agreement, or is there a preferred way of securing the rights to the software?

SAIVAR: The ubiquity of work-for-hire agreements has created an expectation that they should be utilized in any relationship that involves the creation of rights that may be protectable under copyright. What many businesses don't understand is that, under the Copyright Act, there are actually only nine distinct categories of works that can qualify as works-made-for-hire outside of an employment relationship. There is usually a legitimate question as to whether the rights under a software development agreement would fall under one of those categories. Worse yet, a little-known quirk in California employment law causes a contractor under a work-for-hire agreement to be classified as a "special employee" which can impose certain unemployment insurance and workers' compensation obligations on the hiring party. For these reasons, I recommend that most software development agreements should simply include assignment language instead of traditional work-for-hire language.

◆ What criteria should be used in deciding what inventions to patent?

COHEN: I always ask the client "what value" does it have to you and "what are the anticipated changes" to occur in the next few months or years. Further, what is the lifespan of the technology or product, is it long lasting, as in at least a few years, or is it ephemeral? Those high level questions often guides our decision as to whether to file a patent or not, and if we are filing a patent it will help us decide what type of patent to file and the urgency of it, or to leverage the technology into another type of IP protection.

INTELLECTUAL PROPERTY & LICENSING LAW ROUNDTABLE

◆ What are the risks in filing provisional patent applications?

COHEN: There are pros and cons to filing provisional patent applications. In many cases we are able to file a provisional application quicker and often at a reduced rate compared to the utility application. So for many startups or companies that have a high volume of inventions and are unsure of the later follow through of the invention, filing provisional applications serves as a great strategy to further evaluate the merit of the invention in going forward. However, failure to provide and disclose to counsel enough detail regarding the invention can be detrimental in the future, particularly if there is litigation in the future regarding the issued utility patent. The subject matter of the provisional application will come to light and can be used against the owners of the patent, if there is conflicting or insufficient disclosure between the provisional and the later utility application that gained priority from the provisional.

◆ What are the timing constraints in filing a patent application?

COHEN: There are several, but to name just a few, patents must be filed within 12 months from the date of public disclosure. As an example, if there was a sale of the invention or disclosure of it a trade show or even possibly a KickStarter campaign, the period for the 12-month deadline can be triggered. Likewise, there is this concept of "priority" meaning that a subsequently filed patent application can retroactive gain benefit of the earlier filing date of a previously filed patent, if the subsequent patent is filed within a certain time period after the earlier patent. If you fail to comply with these statutory deadlines, you can lose the ability to claim priority or worse be completely barred from filing the patent, or more often, a granted patent may be invalidated in litigation upon the revelation that the it was not filed within one of the statutory deadlines.

◆ Do patent trolls still present a risk to traditional businesses, and what is happening that may affect the future of trolls?

DECARLO: Yes, patent trolls still pose a major risk to businesses, especially in the technology space. The judicial trend to be more flexible with an award of attorneys' fees against the losing party may chill cases that have little merit from being brought, but overall the threat will continue.

◆ Are software inventions still patentable?

COHEN: Absolutely. They were never not patentable, rather the lineage of Supreme Court and Federal Circuit cases, starting with Bilski, have placed a much greater scrutiny on not just software patents but also method patents. Section 101 of the Patent Act sets forth the categories of what is and isn't patentable subject matter. The lineage of cases has attempted to clarify and often muddle what the exact standards or test are to determine patentability such as the machine-or-transformation test in Bilski. But generally the question is whether the software or method is too "manifestly abstract to be patentable". The most recent Federal Circuit decision on the matter came down in McRo Inc. v. Bandai, in which software claims survived a ' 101 challenge. The findings have impacted the Examiners at the USPTO in a recent internal memo instructing them to not over-generalize claims in order to make a rejection. Further, it stated that if the claims recite "rules" or "mathematical relationships that improve computer-related technology by allowing computer performance of a function not previously performable by a computer," the claims can be found eligible under § 101.

◆ What is driving the popularity of patent grant reviews of patents?

DECARLO: Post Grant Reviews are popular primarily because of the relatively low cost of challenging a patent in comparison to challenging a patent in an infringement action in court. Additionally, the legal standard for challenging a patent claim in a Post Grant Review is more favorable to a challenger than is legal standard for challenging a patent claim in an infringement action in court.

COHEN: The increased popularity stems from the ability to more quickly and often less expensively invalidate a patent, which will effectively terminate a potential litigation or lead to a quicker settlement. Post grant reviews (PGRs) have a short timeline, typically lasting more than 12-18 months. By instituting a PGR challenge, patent controversies can be more quickly and efficiently resolved.

◆ What is a business associate agreement, and are businesses in violation of any federal or California laws if they do not have one?

COHEN: A "business associate agreement" is required under privacy standards adopted by the U.S. Department of Health and Human Services for a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. Therefore a business only needs it if they have access to private health information.

◆ Are there any hurdles to consider (pertaining to intellectual property) when one company acquires another?

SAIVAR: It can depend on the industry. I see the biggest IP issues in acquisitions involving emerging tech or digital media companies. These companies have often grown too fast to have focused on legal issues and may have even built their user base playing

INTELLECTUAL PROPERTY & LICENSING LAW ROUNDTABLE

'Businesses need a law firm that is familiar with their field. A firm that already has clients in your field already knows how the business operates and can easily identify and anticipate the pitfalls and common problems before the first meeting. Businesses should also assess the track record, and the size of the law firm to determine if they are the right fit to give them the proper amount of attention. Sometimes new businesses can be lost in the shuffle at larger firms, and the client ends up stalking their attorney to remind them they exist. Communication between the law firm and business is essential. The expectations between the two parties must be made crystal clear from the get-go.'
MICHAEL COHEN

'Budget for and secure enforceable, exclusive IP rights such as patents, copyrights and trade secrets as soon as possible. Conduct regular audits of the company's activities to identify protectable rights and then aggressively perfect those rights by taking the actions necessary to protect each type of right. Too often, companies sacrifice these efforts and end up paying far more later than what they saved early.'
DAN DECARLO

Continued from page 21

fast and loose with intellectual property laws and data security. All of this can cause heartburn for lawyers on both sides of the deal, especially those coming from a traditional entertainment background. Both the lawyers and their clients may need to alter their expectations and traditional contract requirements if they want to get a deal done. At the end of the day, the acquirer may have to accept the warts that come along with what may be an extremely valuable brand and user base and simply understand that they're going to have to clean certain things up going forward.

COHEN: The common hurdles always involve ownership and value of the IP. Double and triple check the paperwork. Additionally, make sure the Patents and Trademarks are filed correctly, and not prone to any invalidity issues in litigation down the road. Don't look at the new company through rose-colored glasses or like a shiny new toy you are about to get. Take an objective approach, and scrutinize everything.

◆ What should a business look for when selecting a law firm to represent their IP or licensing interests?

SAIVAR: At this point, being an expert in only one area of IP law may not be enough to best guide a client with respect to its IP needs, even if the majority of those needs fall within that singular area of expertise. In addition to understanding traditional IP issues involved in registration, enforcement and licensing, I think an effective law firm also needs to have a deep understanding of more niche areas of the law that are growing in importance as the business landscape changes. A firm with an expertise in social media (and the role of influencers within it), e-commerce, FTC regulations and privacy issues can be a major asset to any IP-centric business. Small decisions in one area may have large implications in another so having an IP attorney with a wide breadth of expertise is critical.

COHEN: First and foremost, businesses need a law firm that is familiar with their field. A firm that already has clients in your field already knows how the business operates and can easily identify and anticipate the pitfalls and common problems before the first meeting. Businesses should also assess the track record, and the size of the law firm to determine if they are the right fit to give them the proper amount of attention. Sometimes new businesses can be lost in the shuffle at larger firms, and the client ends up stalking their attorney to remind them they exist. Communication between the law firm and business is essential. The expectations between the two parties must be made crystal clear from the get-go.