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 2017 – from the perspectives of those in the trenches of our region today.

Thanks to our superb panel for their expert insights.
What are some common copyright issues that small businesses face? How can they best be addressed?

SAVARI: In today's world, consumer-facing businesses are tightly concerned with consumer engagement and are therefore feeling pressure to consistently generate content for their websites and social media accounts, even if their core business has nothing to do with content. Often, the people in charge of generating that content grow up thinking that if they can find it online, they can use it or share it without needing a license. This is especially problematic now because technology has made it much easier to find and use excerpts of imagery online; in fact, there's now a cottage industry of law firms that represent photographers or other owners of copyrighted images that send automated demand letters seeking license fees for such uses. It's important for businesses to train their employees (especially the younger ones) that they should never download, copy and paste or otherwise save and upload images they've found in Google image searches or on third-party platforms. If they ignore that advice, the business is likely to receive a demand that may have to be heeded.

The Trademark Office has previously denied some trademark applications as disparaging. We understand that some recent cases have potentially changed that position. What changed?

HOLM: “The Slants” changed the law. Many will find the term demeaning, derogatory and just plain offensive. So did the U.S. Trademark office, when Simon Tam, the lead singer of a rock band using that name, filed an application for a Federal Trademark Registration. The Trademark Office denied his application because it would “disparage … or bring … into contempt or disparage any persons living or dead.”  15 USC § 1052(a). The Supreme Court held that this specific part of the Lanham Act was unconstitutional and a violation of the First Amendment. Matal v. Tam, 582 U.S. ___, (2017).

How is the Trademark Office addressing that change?

HOLM: The Trademark Office will no longer reject a Trademark application because the mark is offensive or disparaging. However, they will continue to reject applications for marks that are “merely descriptive or deceptively misdescriptive” of goods, or if the mark is so similar to an already registered trademark or trade name that it is “likely … to cause confusion, or to cause mistake, or to deceive.”

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

COSTANZO: Nearly 70 percent of U.S. businesses have reported a cyberattack. The actual percentage may be much higher because many cyberattacks are not reported. However, there are severe civil and criminal penalties for failure to report a hack to appropriate regulatory agencies. When large numbers of customers are affected, the law also requires immediate notification to individuals when personal-identifying information is lost. Companies also may be required to provide two years of credit monitoring service, compensation for any damages and a security freeze on the consumer’s credit report. The government may impose penalties, including restitution, following an attack if the business has not taken the proper precautions to encrypt or obscure customer information. Lastly, disruption to operations also may cause a huge financial impact on a business and the burden on smaller businesses is disproportionally higher. Insurance is available to mitigate these impacts.

SAVARI: At this point, almost every business, big or small, needs to worry about data security. While the enormous corporate data breaches make the headlines, smaller businesses should realize that breaches are a daily occurrence with businesses of every size. While these smaller breaches may not lead to claims by the state, they can still be costly because of the steps the business needs to take to comply with the law. California has very specific procedures any business must follow in the event of a breach; we usually recommend that the moment a breach is discovered, business engage services of an attorney or consultant to walk them through the process. At the end of the day, the most important takeaway is that every business that collects information from its customers should have a data breach plan in place beforehand so that they don’t lose valuable time trying to figure one out after a breach.

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

COSTANZO: There are several situations that lead to liability in the event of a data breach. First, the shareholders can bring a derivative claim against management or the board for breach of fiduciary duty in failing to properly discharge their duty to protect the company’s information. There have been very few cases alleging such liability, but as data breaches become more prevalent, I would expect additional cases. Second, we have seen situations where executives sell shares in the company after a data breach occurs, but before it is announced. In addition to the criminal penalties, the company’s shareholders also may assert derivative claims alleging breach of fiduciary duty.

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

SAVARI: Too many businesses, especially in the startup space, become wedded to new trademarks without first consulting with an attorney to ensure the new marks do not come with potential issues. I often see startups choose descriptive trademarks. Under U.S. trademark law, a brand name that describes the goods or services being offered by that business cannot be registered or protected (absent special circumstances). A startup may want a brand name that immediately conveys to consumers what the startup does; however, they may end up with a brand that’s not registrable or enforceable because of its descriptiveness. Another issue is that the new brand may infringe upon a third party’s rights or at least be similar to a pre-existing registered mark that registration will be unattainable. None of this is a big issue if these issues are spotted early on. They become an issue when a company has already put money behind the brand, incorporated it into its pitch materials or released the product under that name. It can be embarrassing, difficult and costly to change the brand at that point. If they don’t change for those reasons, they may end up with a brand that’s infringing or unenforceable which can hurt valuation. For these reasons, it’s best to make sure the brand is clear to use before it is adopted in any meaningful way.

COSTANZO: I see a large number of mistakes involving trade secrets. Many companies fail to sufficiently educate their employees about what constitutes a trade secret. Many employees are confused about what the company owns when they leave and what needs to be protected when dealing with outsiders, such as business partners. Many employees at technology companies believe that they own the intellectual property rights to works that they devised while employed by the company. Then, when they leave the company, they take things with them that they should not be taking, which causes much disruption to both the company and the employee. Companies also fail to document their creation process sufficiently to withstand a challenge to ownership. For example, a company may hire an employee from a competitor and thereafter introduce a similar new product line. In many cases, the hiring company had been working on the technology for a long time. However, without adequate documentation, it cannot effectively demonstrate the chain of the invention.

In the recent past, many patent infringement cases were filed in the Eastern District of Texas even though the Defendants had minimal connection to that District. We understand that recent cases have clarified the law making it more difficult to show that a patent infringement case should be tried in Texas, and increasing the number of patent infringement cases that might be filed in the Central District of California. What was the change?
HOUN: In May 2017, the U.S. Supreme Court clarified that when determining where a patent infringement case can be filed, a corporation resides where it is incorporated. TC Heartland v. Kraft Foods, 581 U.S. __ (2017). Before the TC Heartland decision, two “venue statutes” played a role in determining which U.S. District Court should hear a patent infringement case. The first, specific to patents, says: "may be brought in the judicial district in which the defendant resides ..." (28 USC § 1400(b)). The other, not specific to patents, says: "a corporation is deemed to be a resident where it is subject to the court's personal jurisdiction ..." (28 USC § 1391(c)). Before TC Heartland, patent holders often argued that if an infringer was subject to a District's jurisdiction under § 1391, they also resided in that District under § 1400. The Supreme Court's TC Heartland decision held that "resides" under § 1400 refers to the Heartland TC Heartland of the patent holder. The Supreme Court’s decision held that "resides" under § 1400 refers to the State of Incorporation, and personal jurisdiction under § 1391 is not relevant.

◆ How have the Courts been addressing that change?

HOUN: Many U.S. companies are incorporated in Delaware, and after TC Heartland, the Delaware District Court is seeing a significant increase in the number of patent cases. The Central District of California, located here in the Los Angeles area was already one of the busiest patent courts, and after TC Heartland, it is also seeing more patent cases. A recent decision further held that TC Heartland is a change in the law. This will allow defendants to bring a motion for transfer in previously filed cases even if they had not previously asked for transfer. In re: Micron Tech., Inc. 581 U.S. __ (2017). Before TC Heartland, defendants to bring a motion for transfer in previously filed cases and after TC Heartland, the Central District of California, located here in the Los Angeles area was already one of the busiest patent courts, and after TC Heartland, it is also seeing more patent cases. A recent decision further held that TC Heartland is a change in the law. This will allow defendants to bring a motion for transfer in previously filed cases even if they had not previously asked for transfer. In re: Micron Tech., Inc. 581 U.S. __ (2017).

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

COSTANZO: Many businesses are not sufficiently aware of California's antagonism to noncompete agreements. Essentially, an employer cannot enforce a noncompete agreement against an employee who leaves the company unless the noncompete was signed in connection with that employee's sale of his or her ownership share in a business and the noncompete is reasonably tailored. For example, an enforceable noncompete would restrict the employee from competing in a reasonably defined geographic area for a reasonable number of years. Many companies doing business in California, but headquartered elsewhere, are not familiar with this concept, which is not common in other jurisdictions. Most other states are much more likely to enforce a noncompete. Some states even presume that an employee will use previously acquired proprietary information at a competing business.

SAIVAR: Businesses should understand that the vast majority of non-compete agreements directed at individuals are unenforceable under California law. The state frowns upon any contract term that seeks to impair a person's ability to make a living. CA Business and Professions Code § 16600 provides that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." There are certain narrow exceptions, however, that allow for non-compete involvings a person who is selling his or her business or a substantial portion of it. In that case, it is seen as fair for the purchaser to restrict competition by the very person who was just compensated for selling his or her business and the goodwill associated with it. However, this does not apply to most situations when a company is trying to prohibit the ex-employees from working for a competitor. In those situations, the best a company can do is to remind both the employer and its new employer that the employee is prohibited from using or sharing the former employer's trade secrets with the new company.

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

SAIVAR: I think the most important steps are those taken before a data breach occurs. First, any company dealing in data should consider obtaining cybersecurity insurance, which will kick in if a breach occurs. Next, while every company may not have the money for a full data security audit, companies should, at the very least, have a qualified IT professional review their technological and internal setup to ensure that there aren’t obvious vulnerabilities that can easily be fixed (such as failing to implement available software upgrades or patches). In addition, companies should understand that the biggest risks often stem from third party service providers who touch a company’s data; therefore, it is important to require any third party software or service providers to implement commercially reasonable data security practices. Finally, every company should have a plan in place for how to react to a data breach. They should understand the general steps and, importantly, have the contact information of an attorney or consultant (or insurance provider) whom they can call immediately if they learn of a breach. The earlier and quicker a company reacts to a breach, the easier it can be to deal with.

COSTANZO: Many companies have instituted training programs designed to assist employees in identifying nefarious emails. For example, businesses will send fake phishing emails to their own employees using the same tricks employed by the criminals to see if the employees respond. A good IT department will institute safety measures, such as blocking unknown executable files, automatically installing software updates and security patches on all computers, as well as restricting administrative privileges. During a data breach, the company should do what it can to stop the attack, or at least minimize its impact. An emergency checklist should exist so that someone knows how to contact the head of IT and other executives when they are away from the office. Following a data breach, the business should use a pre-existing plan that it has devised detailing the company personnel that must be contacted as soon as the breach occurs, such as software engineers who can immediately tackle the...
Continued from page 45

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

**SAIVAR:** Many young companies put a little too much importance on obtaining IP registrations. It may be unaffordable for an IP attorney to say this but I think that when a company is young and bootstrapping, they should be more focused on protecting their product than registering their IP. Most early stage companies I deal with here in LA are in the content, e-commerce, SaaS or ad tech fields. While they may be doing something that’s unique in their eyes, it often does not rise to the level of novelty or non-obviousness required for a patent registration. My advice to most early stage companies is that the most important IP registration they should focus on at an early state is their core brand name. Make sure it’s clear and, if so, submit a trademark application for the word mark. In addition to that, they can protect their concept by not sharing it with others until they absolutely have to; and, then, they should only share it after requiring the recipient to sign an NDA. But don’t worry about registering the logo or various slogans. Don’t worry about getting copyright registrations for the code or designs. Don’t worry about patents at this stage. When a company is on a limited budget, their best protection is being first to market with a solid product. Getting caught up in the time, energy and expense of looking into and pursuing various IP registrations takes away from that. Moreover, it may even end up being useless given how often young tech companies pivot.

**HOLM:** There are too many opportunities for a startup to unintentionally forgo valuable IP rights, particularly as related to inventions and trade secrets, and to a lesser extent for copyright if the work is developed by a third party. Selection of a name or mark that is the same as or confusingly similar to a name or mark that is already in use by someone else can also cause a stumble. An early discussion with counsel can help to identify areas for attention before rights are lost.

**COSTANZO:** Early stage companies are usually involved in raising capital and dealing with investors. The investors will be very interested in efforts made to protect intellectual property, such as patent, trademark and copyright registrations. These intellectual assets will often comprise the only asset that the company owns and any preliminary analysis conducted by a potential investor will involve a close look at registrations. Therefore, it is very helpful to have registered IP with the appropriate agency.

**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:** Unfortunately, California has a little-knownmployment law that potentially makes work-for-hire agreements costly. Under these laws, an independent contractor hired under a work-for-hire agreement is treated as a special employee for certain purposes which require the business hiring them to make certain worker’s compensation and unemployment insurance contributions that it otherwise wouldn’t have to under a typical independent contractor relationship. Most businesses are unaware of this and can later find themselves subject to employment-related claims simply because they used a standard work-for-hire agreement that everyone’s used for years. What’s especially frustrating is that, based on the nature of the software, there is often a real question as to whether the work-for-hire doctrine would even apply to the situation (the Copyright Act lays out specific scenarios under which work-for-hire can apply, and software development doesn’t necessarily fall into any of those scenarios). For this reason, I generally avoid work-for-hire language in pure software development agreements and instead simply include an assignment of rights.

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

**HOLM:** At the core, a patent gives the holder a monopoly, and with that monopoly can come increased price, and/or licensing revenue. Most companies pursue patents on features that cover their own products, and can be used to keep competitors out of that same market. A patent portfolio can also be used for defensive purposes, particularly where a competitor has a significant patent portfolio and there is a risk of threat of infringement. If patents in a portfolio can be asserted against the competitor, the competitor may be less inclined to assert their own patents.

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

**HOLM:** International protection of IP is both complex and expensive. While giving advice to clients on protection outside the U.S., I want to understand the scope of their own operations both in and outside the U.S.

**COSTANZO:** International protection of IP is both complex and expensive. When giving advice to clients on protection outside the U.S., I want to understand the scope of their own operations both in and outside the U.S.

**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:** Unfortunately, California has a little-known employment law that potentially makes work-for-hire agreements costly. Under these laws, an independent contractor hired under a work-for-hire agreement is treated as a special employee for certain purposes which require the business hiring them to make certain worker’s compensation and unemployment insurance contributions that it otherwise wouldn’t have to under a typical independent contractor relationship. Most businesses are unaware of this and can later find themselves subject to employment-related claims simply because they used a standard work-for-hire agreement that everyone’s used for years. What’s especially frustrating is that, based on the nature of the software, there is often a real question as to whether the work-for-hire doctrine would even apply to the situation (the Copyright Act lays out specific scenarios under which work-for-hire can apply, and software development doesn’t necessarily fall into any of those scenarios). For this reason, I generally avoid work-for-hire language in pure software development agreements and instead simply include an assignment of rights.

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

**SAIVAR:** I think it’s critical to engage an IP attorney who is business-minded. It is easy for IP attorneys to be too narrowly-focused on only the IP issues while ignoring the bigger picture. The problem is that when it comes to IP, you can always do more. For example, a company can seek to register every brand name, logo and slogan used in connection with a wide variety of goods and services. It can then seek foreign registrations as well. If you look at this only from an IP perspective, this could make sense. Is it better to have more protection than less? Of course. However, the benefits may only be minor whereas the costs can add up very quickly. An IP attorney should have the confidence to talk their client out of spending money that could better be used in the business. This is especially important for early stage companies who have limited budgets. I’d rather have an early stage client spend money on its product instead of building a wide-ranging IP portfolio, all the IP protection in the world does nothing if the product never takes off.

**COSTANZO:** There are several things that are important to look for in a law firm. First, the law firm should have attorneys who understand the type of IP that the company owns. It is not necessary that a lawyer has an electrical engineering degree to represent an electronics company. However, the lawyer should have a sufficient understanding of the technology in order to effectively represent that client in a dispute or in negotiation. If the business is an early stage company, the nature of its legal needs will be broad. It may need patent prosecution counsel, licensing lawyers, litigation counsel, etc. Accordingly, a firm with these areas of practice would be best. Lastly, and most importantly, a company should look for a lawyer who understands the business and the company’s general objectives.

**What should businesses understand about the vast majority of non-compete agreements directed at individuals are unenforceable under California law. The state frowns upon any contract term that seeks to impair a person’s ability to make a living.**

**JESSE SAIVAR**
Intellectual Property Cyber Theft on the Rise

The number of intellectual property (IP) cyber theft incidents for the remainder of the year is expected to increase, according to 50 percent of respondents to a recent Deloitte poll. When asked which category of potential adversary they believe is most likely to attempt theft of their organization's IP, the prevailing percentage of respondents (20.1 percent) answered “employees or other insiders.” Yet, only 16.7 percent of respondents said access to IP is very limited, on a need-to-know basis only.

“While many of us know—or have experienced firsthand—how a cyberattack can severely disrupt business, loss of an asset as critical as IP can be crippling for most organizations,” said Don Fancher, principal, Deloitte Financial Advisory Services LLP. “Managing risks to trade secrets, drawings, plans, or proprietary know-how that drive your organization’s revenue and competitive advantage often includes quantifying how loss of that IP would impact the business, preparing to identify and pursue potential insider threats and guarding prized business assets,” held on September 28, 2016. Poll respondents were from sectors including banking and securities (13.5 percent); technology (8.4 percent); investment management (6.1 percent); travel, hospitality and services (5.0 percent); and retail, wholesale and distribution (5.0 percent).

As cited in the Deloitte Review article, “The hidden costs of an IP breach: Cyber theft and the loss of intellectual property can constitute more than 80 percent of a single company’s value today. And yet, 84.4 percent of respondents to the Deloitte poll collectively feel that assessing the impact of IP loss and managing relationships would be the largest challenges faced by their organization. Sectors expecting a higher than average increase in IP cyber theft in the next year included: Power and utilities (68.8 percent); telecom (68.8 percent); industrial products & services (64.7 percent); and automotive (63.9 percent). Those sectors expecting higher than average insider IP theft attempts included: Automotive (32.2 percent); oil & gas (27.2 percent); and real estate services (26.2 percent).

Tips for assessing the potential impact and protecting against intellectual property loss include:

• Define the critical assets (e.g., facilities, source code, IP and R&D, customer information) that must be protected and the organization’s tolerance for loss or damage in those areas.
• Validate that any partners or suppliers involved in IP creation or utilization collaborate with the cyber risk program.
• Evaluate whether exposing some IP in the public domain may make the organization more subject to attack.
• Consider whether the competitive landscape points to new cyber threats to IP protection.
• Improve cyber resilience to manage brand impact and market position in the event of IP theft.
• Taking a holistic approach toward cybersecurity isn’t just about balancing technical expertise with information technology investments, or about contingency planning. Organizations need to define their cyber risk, up front, in conjunction with their strategic priorities when making decisions on protecting their most critical assets because they recognize what the adverse consequences would be otherwise.

The choice of a lawyer is an important decision that should not be based solely upon advertisements. Polsinelli PC, Polsinelli LLP in California.
Licensing Expo 2018 Selected for Prestigious U.S. Department of Commerce Program, IBP Select

For second year, IBP Select connects U.S. exhibitors with international business, increasing opportunities for growth in new markets

LICENSING Expo, the world’s largest and most influential licensing industry event, today announced that the trade show has been selected to participate in the U.S. Department of Commerce’s International Buyer Program Select (IBP Select) for the second consecutive year. IBP Select is a joint government-industry effort that brings thousands of international buyers to the U.S. for business-to-business matchmaking with U.S.-based exhibitors and connect them with U.S.-based companies. IBP Select will recruit licensees (those seeking to purchase licensing rights), retailers and manufacturers from five international markets—including Canada, India, Ecuador, China and Brazil—to attend Licensing Expo 2018 and connect them with U.S.-based exhibitors interested in breaking into new, international markets. Collectively, these five international markets represent $21.3 billion in annual retail sales of licensed merchandise (according to the LIMA Annual Global Licensing Industry Survey 2017 Report).

“Licensing Expo has long served as the premier meeting place for licensees and licensors, and we feel a responsibility to help our exhibitors identify and develop meaningful relationships that support their business goals,” said Jessica Blue, Senior Vice President, the Global Licensing Group at UBM. “Given the strong positive feedback we received last year, we’re pleased to once again host the IBP Select program and connect our exhibitors with growing international markets that are hungry to engage with their brands.”

“The IBP Select program is specifically designed to connect motivated international buyers with the most compelling U.S. brands, which makes Licensing Expo a natural part,” said Andrea DaSilva, Global Team Lead of Commerce.”

“While the licensing industry is growing rapidly on an international scale, the top 10 licensors in the industry are U.S.-based, and we have no doubt this will add to the draw for our international delegation at Licensing Expo this year.”

As part of the IBP Select program, Licensing Expo will also host a panel comprised of IBP Select delegate leaders designed to explore the latest international trends in the industry. Panelists will address the economic climate in their home countries, what they’re looking for from the U.S. market and their perspectives on the licensing industry as a whole.

Licensing Expo 2018 was selected to participate in IBP Select after a rigorous evaluation process, further solidifying it as the industry’s premiere licensing trade show. Every year, over 5,000 brands showcase more than 16,000 retailers, licensees, manufacturers, distributors and licensing agents from over 67 countries. Licensing Expo empowers brands and exhibitors to find the right partners to expand and transform their businesses and has connected the world’s most influential entertainment, character, fashion, art and corporate brand owners and agents with consumer goods manufacturers, licensees and retailers for more than 35 years.

Licensing Expo takes place May 22 – 24, 2018 in Las Vegas, NV. For more information, please visit: www.licensingexpo.com.