FISHERBROYLES
A LIMITED LIABILITY PARTNERSHIP

Intellectual Property Law Update

NEWSLETTER

IP Law Update July 2015:
Volume 4, Issue 2

info@fisherbroyles.com
www.fisherbroyles.com

Contributors:

Marty Robins
Direct: (847) 277.2580
Martin.Robins@FisherBroyles.com

Alan Wernick
Direct: (847) 786.1005
Alan.Wernick@FisherBroyles.com

Jill Jacobson
Direct: (408) 345.6635
Jill.Jacobson@FisherBroyles.com

R. Mark Halligan
Direct: (312) 607.0102
RMark.Halligan@FisherBroyles.com

We hope everyone has a wonderful summer! Before you take off, please consider these topics that are likely to be useful when you return to the 'real' world:

- Use of provisional patents to reduce cost of protecting inventions;
- Ownership of data from mobile apps;
- New developments in information security and privacy;
- Start-ups must beware of name challenges from big companies; and
- Trade secrets looming larger in sports … and the rest of business

Saving Money on Patent Filings? No Problem!

Are you perfecting an invention or are you trying to gather financing for your project but want to protect your ideas? Filing a provisional patent application may give you some peace of mind and preserve your rights to obtain patent protection for your technology in the future. A provisional application must be converted to a regular, non-provisional patent application within one year if the applicant desires to proceed with it, but it has less formal requirements and may be filed at a lower cost, giving patent applicants some time to decide whether to invest (and how to obtain) the additional resources needed for the non-provisional filing.

Provisional patent applications may be filed without claims (the narrative description of the property right for which patent protection is sought), and the filing fees are very low, $130 for a small entity with less than 500 employees, or $65 for a "micro" entity who meets the income level and other requirements. Attorney fees will likely be lower due to the lack of requirement to draft claims, and informal drawings may be filed, which will reduce or eliminate the cost associated with preparation of formal drawings by a patent draftsperson. Such applications may be used for any type of patentable subject matter.

If an invention is still being perfected, filing a series of provisional applications may be desirable. Once a non-provisional application is filed, it is not possible to add more material to it. However, a series of provisional applications may be filed for up to one year from the filing date of the first provisional, and then all of the provisionals can be rolled into one non-provisional patent filing. Since the U.S. now has a "first to file" patent system, the earlier one gets their ideas on file with the USPTO, the better.

As the invention evolves over the course of a year, additional conceptual material may be added in increments. The priority date for new material will be the date of its incorporation into and filing in a new provisional application. The low cost of provisional filing fees makes this approach feasible.

Another potential advantage of filing a provisional patent application, followed by a non-provisional patent filing one year later, is that it can effectively extend the expiration date of the eventual granted patent by one year, because patent term is measured from the date of the non-provisional filing. This may be important in industries that derive major value from patents at the end of the patent term, such as pharmaceuticals.

A provisional patent application must meet all of the statutory requirements for patentability, a full description of the invention and enough details to teach the public to make and use the invention without excessive experimentation. If filing without claims, care should be taken to provide description that can support future claims. Detailed drawings, even if not in formal patent format, are also desirable. Failure to adhere to these standards may result in a weak or invalid priority date for the provisional filing.

Our patent attorneys will be happy to discuss whether provisional patent filings will be advantageous for you.

Who Owns Data from Your Mobile Apps? You Have Something to Say.

With the explosion of mobile apps as a key marketing tool, both directly and for the data derived from them, it is critical that those using them as a part of their business strategy take appropriate steps to ensure that their documentation and policies support the intended use. We are sometimes asked, 'Who owns data derived from mobile apps and website visits' and 'What can we do with it'? Such data includes, but is certainly not limited to, material such as locational data from the GPS capability of smartphones, web browsing history and transactional history.

For many companies, the answer is critical, because of the direct use of such material in their marketing activity and their interest in transferring the data either to a data broker or in connection with a sale of their business. As evidenced by the very recent Radio Shack settlement discussed elsewhere in this newsletter, regulators are increasingly interested in this topic both from the standpoint of protecting consumers from identity theft and protecting them from unwanted communications.

While the law is still evolving, it is clear that that those collecting data can substantially enhance their position by taking a few actions:

- Provide in mobile app and website privacy policies and terms of use that as between the app user and the app provider, the provider owns all data arising from use;
- Provide for – and comply with - an 'opt in' to all policies and terms of use whereby the app or site user expressly consents to their terms through a dialogue box;
- If you intend to sell data or transfer it with your business, make this clear in your public disclosures;
- Secure the material (physically and electronically) in the same manner that you would other trade secrets;
- If you intend to use such data for direct marketing efforts, such as sending a coupon to the mobile phones of those who are near your location, say so; and
- Strictly comply with your own policies and terms.

FISHERBROYLES
A LIMITED LIABILITY PARTNERSHIP

Those making use of such data would do well to heed the recently filed FTC complaint by the Electronic Privacy Information Center ("EPIC") involving alternative taxi service, Uber, which seemingly relied upon a user opt-out strategy, causing the company to be entangled in FTC proceedings alleging violation of user rights as a result of its tracking and retention of user locations and usage history, EPIC's announcement is available at https://goo.gl/RxGqK0.

Our IP and Technology partners are pleased to work with mobile app developers and marketers on this topic. While early consultation with us is almost always advisable, it is essential here. Failure to obtain timely legal input can result in major delays or complications for proposed transactions and/or involvement in costly, distressing disputes.

Privacy and Information Security: Much Ado Recently

This area has been quite active in recent months, with many developments potentially impacting your business. Among the most important:

- When the bankrupt estate of Radio Shack sought to sell what was left of its business, the Attorney Generals of 38 states became involved with respect to the transfer of customer information. The company and purchaser entered into an agreement with the offices of the Attorney Generals requiring destruction of some material and significant limitations on permissible uses for the rest. While the implications are not altogether clear, it appears that those pursuing significant M&A deals involving consumer information, including without limitation health and financial information, as well as contact information, should anticipate similar restrictions.

- The US Department of Justice, Cybersecurity Unit, recently circulated its suggestions and guidelines for the prevention and handling of data breaches, noting, "The best time to plan such a response is now, before an incident occurs." Of particular interest are the detailed steps for post-incident containment and response. For example, the DOJ suggests electronic imaging of impacted computers as close as possible to detection of the intrusion. This is intended to facilitate pursuit of the wrongdoer.

While the DOJ's suggestions do not have the force of law, we present them for several reasons. First, they simply make sense in their own right with respect to reduction of risk and mitigation of harm from unavoidable incidents. Second, a good faith effort to comply with them is likely to be helpful to your cause in any legal proceedings which do occur, whether they are initiated by a private party or the Federal Trade Commission. They may also facilitate cost-effective procurement of cyber-liability insurance coverage and/or ISO, PCI, or similar third party certification.

The widely publicized data breach involving federal employees and the federal Office of Personnel Management ("OPM") should only increase the regulatory focus on this area and is already the subject of litigation. As such, it is strongly recommended that you obtain input from our Privacy and Technology partners at the planning stages of your ventures.

FISHERBROYLES
A LIMITED LIABILITY PARTNERSHIP

Starting a Business? Check if Your Proposed Name will Draw Fire

A recent opposition filed in the USPTO Trademark Trial and Appeal Board ("TTAB") shows that when a business uses a name which arguably evokes images of an established existing business, the existing business may seek to prevent such use, whether through trademark opposition proceedings or otherwise. The opposition, *Facebook, Inc., v. Designbook LLC*, is an opposition by Facebook against a new company called "Designbook" which, according to the Designbook web site says, "We're a peer-to-peer marketplace for emerging businesses and new products. We connect entrepreneurs, collaborators and investors to stimulate progress in business." The Designbook mark use, at first blush, appears unrelated to the uses of the Facebook mark.

There are other examples of companies comparable to Facebook pursuing opposition in such situations. As trademark owners of well-known marks, these companies have an obligation to "police" their use in order to avoid consumer confusion. If they fail to do so, they risk dilution in the value of their marks.

Our Intellectual Property partners can help to forestall such claims by working with you at an early stage to assess the strength of your proposed mark in the trademark legal landscape, and help to develop alternatives where necessary.

What can Sports Tell us About Trade Secrets? A Lot!

The recent revelations of an FBI inquiry of the St. Louis Cardinals baseball team pertaining to an alleged hacking of the player performance database computer systems of the rival Houston Astros is a useful reminder that IP issues lurk in many unanticipated situations. If the incident occurred, it is likely a violation of the federal Computer Fraud and Abuse Act, which prohibits unauthorized access into the computers of another, and possibly other federal statues as well, and may lead to both civil and criminal sanctions.

Jeff Luhnow, as a Cardinals executive, built a special, trade secret database called "Redbird" to house all of the scouting reports, player information and other compilations of proprietary data from doctors, scouts and coaches and weighted with proprietary algorithms that provides St. Louis with a competitive advantage in baseball operations and talent evaluation. The Astros hired away Luhnow and eventually it leaked out that he had built a similar trade secret database for them called "Ground Control." According to published reports, certain employees of the Cardinals uncovered one of Luhnow's prior passwords and allegedly "hacked" into "Ground Control" to see if Luhnow copied the "Redbird" system or to access similar proprietary data in the "Ground Control" database. Whether Luhnow did take such property may be a basis for a civil suit by the Cardinals (if permitted under MLB bylaws), but cannot under any circumstances justify the alleged response by the Cardinals.

This case illustrates that any business in baseball or elsewhere which internally develops or commissions internal or third party preparation of a customized computer system needs to consider perfecting its claims of ownership vis a vis the developers and users, as well as controlling and monitoring access to the object and source code, and other components, which comprises the computer system.

FISHERBROYLES
A LIMITED LIABILITY PARTNERSHIP

These issues are not unique to the MLB world. A football broadcasting innovation has prompted them as well in a recently filed case known as *Lynx System Developers v. Zebra Enterprise Solutions*, which illustrates the importance of protecting these assets at every stage of the life cycle of the trade secret asset. According to the complaint, Lynx has sued Zebra alleging unlawful schemes to steal technological innovations for the real-time tracking of athletes and game analysis, and the market for those innovations. Lynx's complaint accuses Zebra of misappropriating such technology to support its deal to use the technology in all NFL stadiums, after making a 'low ball' offer to buy Lync.

Last season, Zebra launched the tracking system at 17 NFL stadiums, with a chip designed by Zebra and embedded in the NFL players' shoulder pads. Lynx claims that Zebra was just a supplier, Lynx is the true inventor and owner of the technology, and Zebra stole it. Besides Count 1 for trade secret misappropriation, Lynx's complaint sets forth several other causes of action. The crux of this lawsuit will center on the existence of trade secrets, the ownership of the trade secrets (some of which have been filed by Zebra as patent applications) and the nondisclosure and confidentiality agreements between the parties. Lynx's management of its purported trade secrets at every stage of their life will be a key consideration.

Regardless of the outcome, the case does teach us that once parties enter into negotiations for a corporate level transaction, their breakdown may lead to disputes about technology or other trade secret misappropriation and that seemingly "boilerplate" documentation may loom large.

Another fundamental lesson of both cases is that trade secret issues are often central to the business models and operations of businesses that are not normally thought of as "technology companies." Regardless of the industry, trade secret owners must understand that trade secrets are fragile assets which must be vigilantly protected. We suggest that every company have a trade secret committee that identifies, classifies, and works with counsel to protect trade secret assets.

Our Technology, Trade Secrets and IP partners are pleased to work with you at all stages of the development, exploitation and M&A process to formulate the optimal strategy for avoidance of such disputes.
