FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

NEWSLETTER

IP Law Update: September 2016
Volume 5, Issue 3

info@fisherbroyles.com
www.fisherbroyles.com

Contributors:

Kimberly Booher
Direct: (650) 636.5958
kimberly.booher@fisherbroyles.com

Joseph Manak
Direct: (917) 597.2667
joseph.manak@fisherbroyles.com

Michael Khoury
Direct: (248) 590.2910
michael.khoury@fisherbroyles.com

Geoffrey Goodale
Direct: (202) 261.6644
geoffrey.goodale@fisherbroyles.com

Marty Robins
Direct: (847) 277.2580
martin.robins@fisherbroyles.com

Intellectual Property Law Update

We hope everyone had an excellent summer and is eager to get back to work! To ease the transition and improve your business prospects, please consider these topics that are of great current significance.

- Major decision you may want to make now regarding your trade secret strategy;
- Copyright law: digital content developments;
- Privacy and information security – US and international issues for senior management;
- New Supreme Court patent damage case and its impact on inventors and businesspeople.

New Federal Trade Secrets Law: Choice to be Made Now

For companies emphasizing protection of their trade secrets as a key element of their business model – which should be all companies, irrespective of whether they have a patent portfolio or consider themselves 'high tech' – the new federal Defend Trade Secrets Act of 2016 is a sea change in the legal environment, and probably the business environment. The ability to (i) stop trade secret misappropriation in federal court as opposed to much less efficient state courts; (ii) obtain seizures of goods based upon such action without a traditional adversary hearing and (iii) obtain attorney fee and enhanced damage recovery, greatly strengthens the hand of those relying on trade secrets in addition to or instead of patent protection.

Those wishing to retain the ability to take full advantage in any litigation which may result of the rights granted by the new law must today provide all employees with written notice of their rights to make certain disclosures in a good faith effort to prevent or redress wrongdoing. The consideration of the potential benefits of each alternative will usually requires discussion with an IP lawyer who is well versed in the new law and possibly with an employment lawyer who is versed in whistleblower issues.

Our IP and employment partners are pleased to assist with this process and help you find the approach which is best suited to your situation.

Copyright Law: Focus on Digital Content

Case Makes Clear DMCA Safe Harbor Requires Real Work to Claim …

In a recent case, a Virginia federal District Judge increased the burden for internet service providers with users illegally sharing digital songs or movies. In a key test of the so called service provider safe harbor under the Digital Millennium Copyright Act, Cox Cable was deemed to be liable for its users infringing activity because it took insufficient action to terminate their use rights when apprised by copyright holders of the infringement and was apparently too slow to pass on these notices.

While the holding of this case is not necessarily embraced by other federal courts (and is under appeal to the Fourth Circuit), at a minimum, it means that ISP's seeking to avoid involvement in infringement litigation must take genuine action when presented by copyright holders with formal, credible evidence of infringement such as the takedown notices contemplated in the law. Notices must be promptly passed on and the use rights of those ignoring them must be terminated in a reasonable time. It is difficult to prescribe a specific time frame, but where someone is engaged in repeat infringement, the ISP must remove them from the system without incessant warnings.

It is not clear if this case will be applied to those operating websites allowing user submissions, in the same manner as the above-mentioned safe harbor has been to reduce their exposure for infringing submissions by site users. However, such operators should also be aware that they have some responsibility to deal with infringing posts of which they become aware.

Whether you are a copyright holder concerned about infringing use of your digital materials, ISP or website operator, our IP and litigation partners can discuss the potential ramifications of this case for your particular situation.

<u>… But Copyright Law is not a Harassment Tool Either – Responding to such Notice</u>

You have a business that sells its goods by listing them on an Internet Service Provider ("ISP") website such as Amazon® or Ebay®. One day, you receive a "Take-Down Notice" informing you that the ISP has removed your listings because someone has demanded that the ISP delist or "take down" your goods from the website pursuant to the Digital Millennium Copyright Act ("DMCA"). The Take-Down Notice informs you that the demander claims that your goods infringe her copyrights. However, after looking into the matter, you believe that that no valid claim of infringement exists, or that the person demanding the Take-Down Notice has no copyrights. Further, you suspect that the claims against you were made to gain an unfair competitive advantage, or to extort you into paying money in exchange for the withdrawal of the demand. You are not alone.

Fraudulent takedown demands have become a widespread problem for merchants who offer their wares on the Internet. Studies have shown that many Take-Down demands were made even where the requester does not own any copyrights. Google's Transparency Reports state that approximately 40 percent of Take-Down demands are based on invalid copyright claims. Indeed, abuses of the DMCA process include claims to copyrights in public domain works. To make matters worse, some Take Down demands are spread throughout the Internet by bots.

In general, the DMCA gives ISPs immunity from infringement suits provided they comply with certain procedures. An ISP does not have to decide the merits of a Take Down demand's infringement claim. The ISP need only comply with DMCA system requirements, ensure that demands contain certain specified information, and make prompt notification of the demands. Once a demand is made with the required information, the ISP will delist your goods and notify you of that fact, together with information identifying the demander.

The DMCA also provides a very useful tool for getting your goods back on line – the Counter-Notice. After the ISP informs you that your goods have been taken down, you can send the ISP notification stating that you have a good faith belief that your goods were removed from the site "as a result of mistake or misidentification." Your Counter-Notice will be forwarded to the demander with a notice that your goods will be re-listed within 10 days, unless the demander provides notice that she has filed an infringement lawsuit seeking a restraining order from a court which enjoins you from selling infringing goods on the ISP's site. If no lawsuit is filed, the ISP must put your goods' listing back on the site "not less than 10, nor more than 14 business days following" the receipt of the Counter-Notice.

FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

Privacy and Data Security

General - Responsibilities of the Board of Directors and Senior Management of for-Profits and non-Profits related to Privacy and Security

Directors and officers have fiduciary obligations to ensure the proper operation of the organization. Specifically, in addition to traditional requirements for financial and strategic transaction oversight, there should be oversight to ensure that the organization takes appropriate steps related to the privacy and security of personal information. The obligations of an organization can extend to personally identifiable health information (PHI), consumer financial information such as credit card and account numbers, the electronic and physical records and information maintained by the organization, business continuity and disaster recovery, and the protection of the ability of the organization to conduct business. These are some of the obligations specifically related to cybersecurity:

- Directors need to understand the importance of cybersecurity and its relationship to organizational risk assessment;
- Public company directors need to address their unique disclosure and control requirements, which are becoming increasingly prominent and were very recently the subject of a Wall Street Journal article entitled "Corporate Judgement Call: When to disclose You've Been Hacked;
- Cybersecurity cannot be looked as just an information technology issue, but rather needs to be seen as a component of compliance in general;
- Boards should ensure that they engage and are regularly briefed by those with adequate experience;
- Boards should ensure that management has a risk management assessment process including ongoing monitoring of new legal developments, and should regularly discuss with management the changing level and types of risks faced by the organization, appropriate efforts to mitigate risks including procurement of dedicated insurance coverage, technical measures, plans to address potential incidents, and the plans, staffing and budgets related to each of these areas;
- The risks associated with cyber and related physical threats should be factored into the organization's business continuity and disaster recovery plans, which should be tested and updated regularly;
- Appropriate, specific benchmarks such as ISO 27001-2 or PCI compliance, should be used to assess the efforts of management;
- The issue of cyber risk allocation must be thoughtfully addressed in the covenant/warranty, indemnity and liability limitation sections of contracts with customers and vendors, particularly cloud vendors.

What about nonprofit boards? These obligations exist for nonprofit organizations as well. While legal responsibility of the board members of a nonprofit organization may vary from state to state, members should understand that there has been litigation on exactly the issue of a nonprofit director's liability. Some states allow the nonprofit to provide potential enhanced protection for director and officers through charter and bylaw provisions, while others impose by statute different specific obligations on these persons. Irrespective of legal liability, however, the better practices are for each director to understand and ensure that the organization's plans and actions are appropriate to address these risks in the same manner as for-profit companies.

The federal HIPAA law governing those in the health care field and their vendors imposes specific obligations on covered entities. There are special privacy and security rules associated with PHI. HIPAA rules require covered entities and business associates to implement and maintain security policies and measures to address cybersecurity to some extent in a manner which differs from requirements applicable to other businesses. There is also recent published HHS guidance addressing minimum standards, how to prevent and address breaches and on ransomware.

It is important to understand that many organizations will be business associates under HIPAA even if they are not directly involved in the delivery of health care, and the legal requirements will apply to them. A fundamental element of a compliance strategy in this area is for covered entities to properly determine when business associate agreements are required and ensure that they are obtained.

In today's environment, both regulatory pressure and the requirements of self-preservation make essential, both familiarity with and implementation of what some would consider best practices. Our privacy and corporate partners can help with both.

Cross Border

Anyone who is or may be involved with the transfer of consumer information from the European Union to the US should consider a registration under the newly adopted Privacy Shield. This registration commits the registrant to a number of data and consumer inquiry handling practices agreed upon by the EU and US. It is the successor to, but substantially different from, the previous Safe Harbor. Compliance with the Shield should allow registrants to avert government enforcement action.

Of at least equal importance is the potential gain in marketplace credibility which may be provided by registration. While it is too early to know for sure how things will progress, for many large multi-national companies, it is imperative that they be able to demonstrate to regulators their sensitivity to proper data handling practices. Insisting upon registration by their vendors may be an expedient way to do so … **and give a leg up for potential vendors who possess such status.**

It appears that in most cases, registration will be relatively economical for all registrants, especially for those with prior Safe Harbor registrations, and the process likely to take no more than 30 days to submission once we obtain required information. For companies with prior Safe Harbor registrations, such figures should be less.

It goes without saying that registration is much more than a 'paper exercise' which should be undertaken only by companies with the willingness and ability to ensure proper handling of sensitive materials.

Our privacy and technology partners are pleased to work with you to develop language which is properly suited to each situation whether or not it involves cross-border data transfers.

New Federal Directive

On July 26, 2016, the Obama Administration issued a Presidential Policy Directive on United States Cyber Incident Coordination (the "Directive"). The Directive establishes a framework for responding to cyber incidents pursuant to which threat response will be coordinated by the Federal Bureau of Investigation (FBI), asset response will be coordinated by the U.S, Department of Homeland Security (DHS), and intelligence support and related activities will be coordinated by the Office of the Director of National Intelligence.

The Directive also sets forth principles for federal agencies to use in responding to any public or private sector cyber incident that is brought to their attention. Under these principles, while the Federal Government will coordinate with the affected entities to the extent possible, the Federal Government is provided with the authority to issue a public statement concerning an incident in the event that doing so serves a significant Federal Government interest.

FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

As required by the Directive, DHS and the U.S. Department of Justice (DOJ) have created a fact sheet outlining how private individuals and organizations can contact relevant federal agencies about a cyber incident (the "Unified Fact Sheet"), which can be accessed at: www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf. The Unified Fact Sheet notes that, upon receiving notification of a cyber incident, the Federal Government will focus on threat response and asset response, and accordingly, as discussed above, companies that provide such notification must be aware of and prepared for the FBI, DHS, and possibly other agencies, becoming involved in the matter.

While the Directive establishes a framework for coordinated response by the Federal Government to cyber incidents, companies should carefully evaluate whether to contact Federal agencies when a cyber incident occurs and how best to do so. Our Privacy and Data Security partners can assist in evaluating all relevant factors and designing and implementing an effective cyber incident response strategy.

Patents: Easier to Obtain Enhanced Patent Damages

As noted in our last Newsletter, the US Supreme Court recently determined that a plaintiff who succeeds in establishing willful infringement of a valid patent should face a reduced burden for recovery of not only actual damages (and entry of an injunction), but also attorneys' fees and enhanced damages of up to triple the actual damages. In a nutshell, plaintiffs no longer need to satisfy any standard of proof other than the traditional civil 'preponderance of the evidence' test, and the egregious nature of the defendant's actions will have nothing to do with the defenses which they put forth at trial.

This changes the analysis for both patent-holders who seek to redress infringement, but also those considering a challenge to an existing patent or who have been advised to cease and desist in their conduct. While a patent-holder is still inviting a probable challenge to their patent's validity when they sue for infringement, the Court's holding improves their potential return if they are successful in their defense of the patent and demonstration of its infringement.

Our patent and litigation partners can elaborate upon potential ramifications of this case for your specific situation.