NEWSLETTER

IP Law Update: December 2015
Volume 4, Issue 4

info@fisherbroyles.com
www.fisherbroyles.com

Contributors:

Kim Booher
Direct: 650.636.5958
kimberly.booher@fisherbroyles.com

Susan Freedman
Direct: (703) 237-1282
susan.freedman@fisherbroyles.com

R. Mark Halligan
Direct: (312) 607-0102
rmark.halligan@fisherbroyles.com

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

Alan Wernick
Direct: (847) 786.1005
alan.wernick@fisherbroyles.com

FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

Intellectual Property Law Update

We hope everyone is having a wonderful holiday season and has a wonderful new year! To improve your business life, please consider these topics that are of great current significance:

- Judicial consideration of Washington Redskins' trademark registration cancellation;
- Developments in information security and privacy regulation;
- Need for good information security practice to support trade secrets;
- Cautionary steps associated with use of open source software; and
- Potentially new recourse for copyright owners concerned with infringement

Redskins Seeking Replay Review of Trademark Decision

The NFL's Washington Redskins filed their long-anticipated appeal brief to the U.S. Court of Appeals. The team seeks to overturn the district court's action cancelling six of the team's REDSKINS trademarks registered between 1967 and 1990 as "disparaging" to Native Americans.

The Redskins seek to have the court hold that the USPTO and the district court wrongly denied the argument that the content and viewpoint restrictions of the "disparagement" clause violate the First Amendment, by cancelling registrations that convey messages the government disfavors. The Redskins ask the court to find the disparagement clause unconstitutionally vague. Whether a trademark disparages a "substantial composite" of a group like Native Americans is wholly subjective, and fosters arbitrary enforcement. As a result, the government's decisions on disparagement are arbitrary and unpredictable: Arbitrary enforcement of the disparagement clause led to the unprecedented cancellations of the REDSKINS trademarks in this case.

The team also appeals the lower court's ruling that the government's "massive" delay in cancelling the registrations did not violate due process because by 2006, when the Native Americans sought cancellation, the best evidence of what Native Americans thought in 1967 was long gone.

On the issue that the Redskins marks were not disparaging when registered starting in 1967, the Redskins claim that the Native Americans failed to show, by any preponderance of the evidence, that the REDSKINS marks were disparaging when registered in 1967, 1974, 1978, or 1990, the dates of registration.

On the issue that delay bars the cancellation claim, the Redskins argue that the district court erred in finding that laches did not bar the petitioner's cancellation claims. Since the oldest petitioner waited six years while the youngest waited 11 months and 20 days, the delay economically prejudiced the team because during 2006, the value of the team's brand grew $18 million to $130 million.

In light of this case, trademark owners should be particularly careful when selecting trademarks that might be deemed "disparaging." It is best to err on the side of selecting trademarks that might not be viewed in this light. If you are considering selecting a mark that might be viewed as "disparaging," our trademark partners our trademark partners are happy to provide advice.

Privacy and Security: PCI's, Class Actions, Cookies and Safe Harbors

Wyndham Hotel Data Breach Order: 20 Years, PCI Standards and Franchise Oversight

In its widely followed Wyndham Hotels case, the FTC entered into a settlement agreement which will be in effect for 20 years and, among other things requires use of the Payment Card Industry Data Security Standard ("PCI DSS") security standards for credit and debit card transactions, annual reporting to the FTC of third party audits of Wyndham's compliance with the FTC approved standards, and imposes special obligations on franchisors and franchisees. While the settlement is by its terms applicable only to Wyndham, it is quite instructive for companies seeking to avoid entanglements.

Privacy Issues Becoming a Class Action

A recent federal appellate case involving Google underscores the need for companies to be truthful and open about their practices involving use of customer browsing and related data. Pending potential US Supreme Court appeal, the plaintiffs are allowed to maintain a class action lawsuit against Google as a result of its alleged undisclosed overriding of user "cookie blockers" to access internet history information, which was presumably used by Google and its advertisers to target web advertising in violation of California privacy laws.

A class action is quite risky for defendants in terms of potential damages and is usually settled on costly terms in view of such exposure. This is one of the few cases in which such status has been obtained as a result of allegedly inappropriate practices in the security or privacy areas. If the case is a precursor to similar treatment in the area by other courts, this raises the already high stakes associated with practice and disclosure in the area.

Making the case even more noteworthy is the fact that it did not involve any fraudulent activity resulting in economic loss to anyone. This illustrates the important distinction between security and privacy and the importance of ensuring proper practices in both areas. Rapidly changing state laws and FTC policies regarding tracking of internet browsing and mobile app location data make it essential to work closely with counsel to facilitate compliance.

A complaint very recently filed with the FTC against Google involving its Google Apps for Education service also illustrates the exposure. Even though no one suffered any financial loss, the complaint alleges that Google failed to adhere to its pledge to use data collected through such apps only for educational purposes. There is substantial and increasing scrutiny on companies' privacy practices, which must be addressed separately and to the same extent as information security.

EU-US Data Transfers Absent a Safe Harbor

As to the latter, as has been widely reported by us and elsewhere, the Safe Harbor framework for certain data transfers (of personal information) between the EU and US was struck down in October by the EU Court of Justice. On January 31, 2016 the "grace period" for data flows from Europe to the US previously permissible under the Safe Harbor framework comes to a close. At such time, data practices may come under scrutiny, and many companies are at risk of enforcement actions by the various EU Data Protection authorities. As has been discussed, potential alternatives to the Safe Harbor (for large-scale and regular data transfers) include Standard Contract Clauses and

Binding Corporate Rules prescribed by the EU, but some authorities in Europe have questioned these alternatives as well.

We are monitoring developments about a new Safe Harbor agreement that has been in the works since Edward Snowden's revelations in 2014. The European Union Commissioner for Justice met with US officials last month to discuss cross-border data transfers and to continue negotiations of a new Safe Harbor agreement. There are some officials who believe that the new Safe Harbor framework could be in place by the expiration of the January 31, 2016, grace period. We cannot recommend a "wait and see" approach. Rather, we will closely monitor developments, and in the meantime encourage continued efforts toward permissible data flow mechanisms under the current framework and welcome discussions with you toward that end. In the same vein, in addition to use of prescribed contract clauses in major agreements, we suggest consideration of relocation of servers and/or processing of the most sensitive data to the EU. Our Privacy and Data Security lawyers are pleased to assist you in developing and implementing privacy and data security practices and policies and with your contract negotiations.

Trade Secrets Must be Kept Secret

Those interested in securing their company's trade secrets – which should be all readers – need to remember the importance of good information security practice. Under applicable law, material qualifies as a trade secret only if its owner utilizes reasonable measures to keep it secret.

This involves identifying and enumerating such materials. They are often customer, supplier and employee lists, and know-how such as product formulas, operations manuals and customer pricing and purchase history. It involves material that offers a competitive advantage to its user but is not subject to patent protection, whether because of owner choice or legal unavailability. Even companies not viewed as high tech in nature invariably have several trade secrets.

Once the material is identified, it must be properly secured. While, this often involves written agreements and policies requiring confidentiality, this is only a starting point. Affirmative security measures are needed.

This means not only physical security such as locking file rooms, but also electronic security such as use of firewalls, intrusion detection hardware and possibly encryption, and limiting access to those with a need to know through electronic partitioning of databases and disabling USB ports where possible to prevent disgruntled employees or visitors from walking off with it. Trade secret disputes arise from both 3rd party hacking and employees walking off with sensitive material on paper or flash drives or sending via e-mail, when joining competitors or starting their own businesses. Both types of exposure must be properly addressed through technical and policy measures.

For public companies – and probably private companies raising money in private placements – the SEC requires disclosure of steps taken to secure such materials and an evaluation of the risk of their misappropriation. Our IP and privacy partners can work with you to craft a trade secret and data protection strategy that fits your company's specific circumstances.

Open Source Software: Usually Cash-free, but with Strings Attached

While everyone knows of the need to comply with contractual terms in software licenses (and elsewhere), the salient point in this context, is that under several recent cases, failure to do so with respect to a license for copyrighted

FISHERBROYLES®
A LIMITED LIABILITY PARTNERSHIP

material (which is usually applicable to software), allows the pursuit in United States District Court of claims for infringement damages under the Copyright Act and related items, such as attorney fees. This is in addition to traditional contract damages, which may be non-existent or difficult to prove. For example, if the evidence establishes (among other things) that the work infringed was a registered work in the U.S. Copyright Office and the infringement was willful, then the court may, in its discretion, award statutory damages of up to $150,000 (regardless of the retail cost of the underlying work).

As licensees of computer software, you should understand that compliance with the letter and spirit of licenses is essential, notwithstanding the apparent absence of substantial actual contractual damages from non-compliance. Infringement damages are likely to be quite substantial. As licensors of computer software, you should be aware of potential leverage that the cases and statutes provide where bona fide non-compliance is found.

Critically, the preceding analysis applies not only to customarily negotiated and executed licenses for proprietary computer software, but also to "open source" software ("OSS"). While OSS is increasingly a cost effective alternative to traditional proprietary software, and we encourage our clients to explore its use, it carries with it binding contractual obligations, which must be identified and complied with. In our practices, we continue to observe a large number of cases where OSS product is embedded in proprietary software. The foregoing suggestions concerning non-OSS works are applicable in these cases to the same extent as in "pure" OSS situations. Licensees should make sure that licensors tell them what OSS product, if any, is being embedded in what is being delivered, while OSS licensors should monitor the use of their products in this context. A brief article by a FisherBroyles' attorney discussing OSS is available at http://tinyurl.com/OpenSource2008.

Copyright Holders May Have New Enforcement Tool

Those concerned with frequent digital piracy of their copyrighted content may have additional leverage. A very recent ruling by a federal district judge in a case involving Cox Communications indicates that if internet service providers do not take meaningful action to terminate the access of those identified by copyright holders as "repeat infringers" who are frequently downloading digital content without payment, the ISPs may be liable for large statutory damages.

While the case has yet to be tried in full and is likely to be appealed no matter the outcome at trial, if the ruling stands, it provides significant leverage to copyright holders who feel that their rights are being violated by individuals who are likely difficult to find and usually judgment proof.

If you are such a copyright holder, our IP partners may be able to assist you with measures to protect your interest.

Founded in 2002, FisherBroyles, LLP is a full-service, cloud-based national law firm with attorneys across the country. Conceived as the "Next Generation Law Firm®", FisherBroyles eliminates unnecessary overhead that does not add value to clients and instead offers a more cost-effective solution to clients across all industries. Visit our website at www.fisherbroyles.com to learn more about our firm's unique approach and how we can best meet your needs.