

Brand Protection is an App-solute Must

David Bell¹ and Hope Hughes²

The ubiquity of mobile and Internet applications, or apps, is astounding. Because the mobile apps market will continue to have an increasingly significant impact on the global marketplace, intellectual property practitioners should familiarize themselves with trademark and copyright issues that apps raise and methods of addressing those issues.

WHAT'S 'APP-ENING

One can download apps for social networking, games, navigation, translation, weather, travel itineraries, music and video streaming, photography tools, and for virtually any other use or category one can imagine. The mobile apps market is a serious business, though – indeed, it is a multi-billion dollar business projected to generate \$25 billion by 2015.³ A recently released free app called Color, which facilitates location-based photo sharing, raised a whopping \$41 million in venture capital before its release.⁴

Apple's App Store is expected to contribute nearly a quarter of projected revenues in the next few years,⁵ but also vying for a piece of the apps pie are competitive marketplaces (also called platforms), including Google's Android Market, Amazon.com's Appstore for Android, App World for BlackBerry, Windows Phone MarketPlace, Palm's App Catalog, Nokia's Ovi Store, and the Samsung Application Store. Although mobile apps are geared for use on mobile devices, apps are not limited to use on such devices. Google's relatively new Internet browser, called Google Chrome, is a social-oriented browser that features apps.

Further illustrative of the proliferation of the business, companies have begun litigating over the branding rights to their platforms. Apple has aggressively attempted to stop others from using the phrase "app store," which Apple uses to identify its online store and from which it offers apps for its iPhone, iPod Touch, and iPad devices. On March 18, 2011, Apple sued Amazon.com in California federal court over use of the name "Appstore for Android",⁶ and days later Apple sent a cease and desist letter to MiKandi, the self-proclaimed "world's first app store for adults."⁷ Apple has also pressured Microsoft against using the term, and Microsoft fired back by opposing Apple's U.S. trademark application for APP STORE on the ground that the term is generic.⁸

¹ David Bell is a partner in the Dallas, TX office of the law firm of Haynes and Boone, LLP. His practice emphasizes trademark and brand counseling, prosecution, and enforcement. He may be reached at david.bell@haynesboone.com or 214.651.5248.

² Hope Hughes is an associate in the Dallas, TX office of the law firm of Haynes and Boone, LLP. Her practice emphasizes trademark and brand counseling, prosecution, and enforcement. She may be reached at hope.hughes@haynesboone.com or 214.651.5033.

³ Mobile App Market: \$25 Billion by 2015, ReadWriteWeb, <http://www.readriteweb.com/mobile/2011/01/mobile-app-market-25-billion-by-2015.php> (last visited Apr. 5, 2011). People use their cell phones more for data than making phone calls. Jenna Wortham, Cellphones Now Used More for Data Than for Calls, N.Y. TIMES, May 13, 2010, <http://www.nytimes.com/2010/05/14/technology/personaltech/14talk.html> (last visited Apr. 5, 2011).

⁴ Color: The \$41 Million Dollar App Is Released, APPADVICE, March 25, 2011, <http://appadvice.com/appnn/2011/03/color-41-million-dollar-app-released/> (last visited Apr. 5, 2011).

⁵ ReadWriteWeb, *supra* note 1.

⁶ Apple Inc. v. Amazon.com, Inc., No. 11-1327 (N.D. Cal. Mar. 18, 2011).

⁷ Apple sends adult app store cease-and-desist order, CNET NEWS, Mar. 23, 2011, http://news.cnet.com/8301-13579_3-20046191-37.html (last visited Apr. 5, 2011).

⁸ Microsoft Corp. v. Apple, Inc., T.T.A.B., No. 91195582, motion for summary judgment filed 1/10/11.

A BAD APP SPOILS A BUNCH

Apps can raise a number of copyright and trademark infringement concerns. For example, company names, product and service names, logos, and copyrighted content are often used in the names, icons, summaries, and content of apps without the rights holders' consent.

Additionally, poor quality apps present several problems. At best, a simple app that might merely consist of a link to a website, may function as intended but result in unimpressed and disappointed consumers, or might fail to forward users to the desired website. More complex apps may fail to work due to poor programming, or may cause user devices to crash. Consumers who encounter unauthorized branding on substandard apps will likely form negative opinions of the brand owners if they believe the apps are associated with the brands.

While app developers that incorporate others' trademarks may include disclaimers in the app descriptions as to an affiliation with the trademark owner, such notices are unlikely sufficient to remedy all likelihood of confusion issues, as consumers who download those apps may not see the disclaimers.

Then there are scheming developers and hackers, who constitute a more insidious problem than simply faulty or infringing apps. For instance, illegitimate app versions (i.e., counterfeit software posing as valid apps) may be offered on platforms where they should not exist or even on the same platform as valid apps, and such apps may contain viruses that infect user electronic devices and stored content.

Additional insidious problems that plague app users include data theft, data or web scraping, and phishing. Data theft may be accomplished by an app that requests an individual's user name and password, then allows the app developer to capture and store those login details for future illegitimate use. Such data theft constitutes phishing when the app appears to be provided by the users' bank, such that the users believe they are providing information to their actual bank. Data or web scraping consists of extracting information from websites. An app automatically collects information from the brand owner's website, and the app developer may use that information for improper purposes, such as to create a program that mimics the brand owner's app.

The above examples present several trademark and unfair competition concerns as a result of brand owners' trademarks being used without authorization. When a brand is well-known or famous, the brand owner may have a dilution claim even when a likelihood of confusion claim would be difficult to prove. A plethora of phony apps can weaken a brand owner's trademark, while most of the above-described activities also would certainly degrade or tarnish it.

Copyright infringement tends to be more prevalent in certain app categories, with copycats particularly targeting game and MP3-related apps. Yet, with some app developers incorporating portions of brand owners' websites into their own apps or associated materials, and possibly improperly accessing the software or content of the brand owner's own site, both copyright and trade dress infringement are often in play.

ADDRESSING APP MISUSE

In the current landscape, brand owners should generally address infringement with respect to apps as they do in any other Internet or brick and mortar and contexts. While the platforms have changed, the rules of enforcement and IP laws have not.

Monitor platforms proactively.

Brand owners should strongly consider monitoring across multiple platforms for possible intellectual property infringement. As is typically the case with addressing infringement, promptly identifying and taking action against infringing apps is paramount. Consider the more traditional infringing website or physical store: If a demand letter is sent and the website is deactivated or the store's name is changed, then the future harm may be minimal in many cases. While some lingering advertisements and references may continue to pose a problem, the actual infringing establishment will no longer exist or will have changed its name.

In contrast, when an infringing app is deactivated, at least two possibilities remain depending on the platform, neither of which is a great outcome for the rights owner. The app may either still reside on the devices or webpages of those consumers who had previously downloaded it such that the consumer will continue to see the infringing content, or the app may no longer work on those devices or webpages such that consumers who downloaded (and possibly paid for) that app may become frustrated with the brand owner. Thus, the need for prompt action is often heightened in the app space.

Fortunately, brand owners may institute any of several monitoring procedures. For example, a member of the legal or marketing team of the brand owner, or the company's counsel, can regularly review platforms for infringing apps. Most app marketplaces are readily searchable online.

Admittedly, monitoring a large number of platforms and repeatedly taking action by dispatching notice or demand letters can become time-consuming and costly. Many brand owners may elect to take action only after receiving a customer, employee, or executive complaint about a problematic app.

Occasional monitoring is, nevertheless, significantly more effective at protecting a brand than conducting none at all. Brand owners should consider, at a minimum, monitoring quarterly or semi-annually the most popular platforms (e.g., Apple's App Store and the Android Market).

Also, brand owners may create and implement procedures for employees to inform their legal departments about problematic apps that they encounter. This may involve providing a chart in which employees can list the app, relevant platform, specific problems, and information about the developer including contact details and any affiliation with the company.

Some trademark service vendors, including MarkMonitor and Corporation Service Company, offer solutions to monitor multiple platforms and advise the brand owners of potential concerns.

Contact the app marketplace operators.

Upon learning of an infringing or otherwise problematic app, brand owners should consider sending a notice letter with a take-down request to the platform operator. In the authors' experience with contacting the App Store, the Android Market, and the Chrome Store, prompt responses have been received, typically followed by permanent deactivation of apps upon receipt of good faith and detailed notifications of trademark, copyright, or data privacy concerns. It is also productive in such take-down notices to point out any of the rogue developer's violations of the platform's terms of use. However, brand owners should exercise caution when exercising take-down requests as their overzealous use may prompt a legitimate developer or possibly users to sue.

Contact the developers directly.

The app developers' names, websites, or other contact details are typically available in app marketplaces. Some further investigation may be necessary to find accurate contact information, but at least legitimate app developers usually want to be found.

The authors have enjoyed mixed success when dealing with such developers. While most agree to quickly fix or deactivate their apps, on one occasion the developer continued to submit revised versions of their problematic app to a platform operator without resolving the brand owners concerns, requiring contact with the platform operator to refuse the app entirely.

Consider public relations before taking aggressive action.

A risk always exists that dispatch of a legal notice will backfire. For example, a brand owner may be concerned about an icon used for an app, but may not be otherwise concerned about the app's name or content. In such a situation, it may be better to directly reach out to the developer to politely request the icon change, as contacting the platform operator may result in deactivation of the app altogether. That could cause more frustration to the developer (and potentially your client's customer base) than was necessary.

COUNSELING APP DEVELOPERS AND MARKETPLACE OPERATORS

Many companies now contemplate the release or sponsorship of apps to better communicate with and reach their audiences and potential customers. Developing apps, and even operating app marketplaces, can make profitable business and marketing sense.

Always advise your clients to be careful about using others' marks, even when certain nominative or trademark fair use defenses may allow for your client's use of a mark in the app itself, its description, or even in the app name in some circumstances.

Companies setting up their own app marketplaces should be advised to implement a copyright take-down policy per the Digital Millennium Copyright Act ("DMCA"). They should also be advised to consider establishing a policy for screening apps for trademark and other public relations considerations (e.g., for adult or offensive content).

In some courts, the more hands-off the company operating the app marketplace is, the easier it might be for it to defend against contributory infringement claims under trademark law or copyright claims. Yet, app marketplace owners that take a more active role in screening apps for obvious intellectual property and other problems and responding appropriately to take-down requests will be better positioned to avoid litigation altogether and, in some cases, to disprove liability, at least in regard to trademark claims. Thus, with some exceptions, it might be wise for app marketplace operators to emulate operators of websites such as action sites, domain registrars, and social media websites.

CONCLUSION

Use common sense and counsel your clients to follow a few simple rules with respect to apps:

1. Establish and implement a monitoring methodology that makes sense for the business.
2. Consider the issues raised by unauthorized apps, including the potential public relations ramifications of taking any action.

3. Send appropriate notices to developers and platform operators of apps that exceed the client's tolerance point.
4. Clients need not fear entering the app space, but should do their research, and apps should not incorporate others' IP unnecessarily and without permission.

Disclaimer: The opinions expressed herein are the opinions of the authors only and do not necessarily reflect the opinions of the law firm with which the authors are associated, or any of its other attorneys or clients.