THOMSON REUTERS

Westlaw®

Intellectual Property Considerations and Protectable Content in Mobile Apps

Neel Chatterjee and Natasha Daughtrey*

JUNE 7, 2018

Everyone has heard the story of how Facebook started. A few young kids had an idea for a social networking website and launched it from a college dorm room into what quickly became one of the most valuable companies in the world with billions of users. Today many of those users access their Facebook accounts not from traditional computers, but from the Facebook application on their cellphones. Indeed, there are a stunning 1.45 billion people in the world who access the Facebook application every day. It's not just Facebook that is being downloaded onto mobile devices, the average person uses nine mobile applications *per day*.

Countless companies have tried to get in on the action by developing mobile applications from simple entertainment games to complex apps managing finances and healthcare records. Companies also develop customized mobile apps for their businesses. Some mobile apps become enormous hits (like Angry Birds, Spotify, and Words with Friends) with sustained followings and cash flow that provide the mobile app with a long term recurring revenue. Others may take off at first, but are quickly overwhelmed by copy-cat competitors that lure users away and dilute the value of the original mobile app. And many more applications never gain traction at all. Below we discuss the challenges mobile app developers face when trying to protect against intellectual property and data theft. We specifically discuss how mobile applications can be developed in ways that will increase the likelihood of being able to protect against follow on "copycat" apps, and lifting of user-generated content on mobile apps.

The starting point of any intellectual property protection scheme should start with the following question: What is the core value of the asset you wish to protect? In the mobile app context, the core monetization strategies fall into roughly four categories: (1) paid apps, (2) in-app purchases, (3) in-app advertising, and (4) monetization and use of user data and content. User experience in a mobile app (and particularly in gaming apps) can be drivers of these monetization strategies. Historically, user experience has been elusive in terms of intellectual property (hereinafter "IP") protection.

The second question to ask in developing an IP protective scheme is what are the business objectives of IP protection for the company? IP protection can serve multiple goals. The most common goals for mobile app developers is to protect against copycat apps and/or data theft. A secondary goal can be to develop defensive strategies should a competitor assert a claim.

The third question to ask is: In what venues will the mobile app be relevant? Mobile apps often work in various ecosystems such as Facebook, the Apple store, and Google Play. The mobile apps may also focus on particular countries. The venue can materially impact what IP strategies to employ and dramatically affect the cost of seeking protection. For example, if you are working in a particular ecosystem, each ecosystem has its own unique approach to resolving IP disputes within the ecosystem. All of them have reporting mechanisms for IP issues. The ecosystems will sometimes act when questions of consumer fraud or data privacy are implicated. However, the ecosystems will only go so far in resolving IP disputes and often will want competing apps to work out their differences directly.

In terms of concrete strategies, mobile app developers have several tools to protect their apps against would-be competitors, including patent, copyright, trademark, trade secret, and data protection laws. Each type of IP strategy differs in how the rights are obtained, what they protect, and how they can be enforced.

• **Patents:** The broadest form of protection of an invention is a patent because it prevents others from practicing the invention described in a patent and equivalents of it for 20 years from the date of issuance. It is time consuming and expensive to obtain a patent, and patents are unavailable for mobile apps that are not inventive over all prior disclosures and apps. Also, some patent applications must comply with 35 U.S.C. § 101, which states that patents may only be granted for a "useful process, manufacture, composition of matter or machine." In the current patent climate, the Patent and Trademark Office often rejects applications directed to an "abstract" idea for a game or application that merely uses a computer or cell phone to implement it. However, innovative technologies, such as personalized emoji from a camera phone, may have innovations that are technical in nature and therefore patentable. Cases evaluating the patentability of game mechanics and mobile apps are very sparse, and there is some unfavorable case law regarding patent protections for graphical user interfaces and user experiences.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

the answer company™
THOMSON REUTERS®

• **Trademarks:** A trademark protects the name or logo of the application or company so long as they are in use and do not lose their association with a specific good or service. These can be enforced against a competitor that uses your app's name (or anything confusingly similar to it) in selling an app. Many people claim that the "look and feel" of the app experience can be protectable as "trade dress" when another copy-cat app is so similar that users may be confused as to the actual app creator. While some games and distinctive user interfaces have been found to be protectable, the evidentiary hurdles showing a likelihood of confusion and nonfunctional distinctiveness can be significant.

• **Trade secrets:** Trade secrets protect information, such as algorithms or technology that is kept secret and is valuable because it is secret, and lasts so long as it remains a secret. This protection is useful for the "secret sauce" of a mobile app. Trade secrets are often created and maintained through non-disclosure agreements with employees and vendors. On the other hand, to claim trade secret protection, a plaintiff needs to prove that a competitor obtained access to the trade secret through an NDA, theft, or other relationship. If someone can reverse engineer your trade secret – you don't have any recourse against them.

• **Copyright:** Copyright protects the nonfunctional expression in a mobile app. A game character, imagery, and creative visuals and/or sounds can all be protected. The underlying code for the mobile app is also protectable. Registering a copyright is an inexpensive way to obtain long term coverage (95 years from first publication and 120 years from creation) of these aspects of a mobile app. While it prevents others from using the same materials, it can also cover the structure, sequence, and organization of storylines, code, and other expressive elements. There are several defenses to a claim of copyright infringement including fair use and independent creation. Thus, having a copyright will not necessarily preclude others from taking your content and transforming it, or from having the same or similar content to your copyrighted content if it was independently created.

• **Terms of Service/User Policies**: The value in some mobile apps is based on the volume of user-generated content on the app. For example – having more people "pin" boards in the Pinterest app likely increases the number of people who download the app so they can view those boards (and maybe pin some of their own boards). This increases the app's value. Thus, in addition to traditional intellectual property law protections, it may also be prudent to protect content placed on your app from app users or other third parties. Carefully drafted terms of service or user policies can prevent competitors from taking user content on your application and putting it on their own app or otherwise using your application in a way that diminishes its value. Terms of service and user policies can be the basis for claims of breach of contract or fraud.

• **Computer Trespass Laws and the Digital Millennium Copyright Act:** The Computer Fraud & Abuse Act (18 U.S.C. § 1030), state computer trespass laws, and possibly the Digital Millennium Copyright Act (17 U.S.C. § 1201), are helpful tools to protect data and user generated content used by or stored through a mobile app. Unlike protection of the app itself, these laws protect against intrusions where competitors or hackers try to take content from your app for anti-competitive purposes. These laws will not necessarily stop copycats, but they will prevent valuable data theft.

One recent dispute involving several of the above strategies illustrates the benefits of employing a broad protection strategy for mobile apps. Ticketmaster operates one of the largest live event ticket selling businesses through a website and mobile app. Because demand often exceeds supply, Ticketmaster has measures in place to regulate the number of tickets that can be purchased through its mobile app at one time. Indeed, consumers expect and rely on Ticketmaster to have a fair and equitable way of distributing tickets to high demand events. To achieve this, Ticketmaster's terms of use and code of conduct (hereinafter "TOU") restrict the number of tickets an individual can buy and do not allow the use of automated programs or "bots" to exceed the ticket purchase limits. The site and mobile app also use CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") technology to prevent bots from buying tickets. The TOU provides a limited license to customers to view the site, and states that a violation thereof constitutes a reproduction or display of the site and infringes Ticketmaster's "copyright, trademarks, patents and other rights in the Site and Content."

Ticketmaster sent a cease a desist letter to several related companies who allegedly used bots to purchase over 300,000 tickets for events using 9,000 accounts and then resold the tickets on third party platforms for profit. According to Ticketmaster, these companies used bots to purchase up to 40% of any given tickets for the Broadway stage play *Hamilton*, and the majority of the tickets for major sporting events like the Mayweather v. Pacquiao boxing match in Las Vegas. These sophisticated bots also avoided Ticketmaster's CAPTCHA system and other anti-bot systems. When the companies continued their activities despite the cease and desist letter, Ticketmaster sued for claims including breach of the TOU contract, copyright infringement, violation of the Digital Millennium Copyright Act (hereinafter "DMCA"), fraud, violation of the Computer Fraud and Abuse Act (hereinafter "CFAA") and a similar state law, and violations of anti-scalping laws. Ticketmaster L.L.C., v. Prestige Entm't, Inc. et al., No. 17-cv-7232 (C.D. Cal.). Ticketmaster alleged that it was harmed by defendants' actions, which strained Ticketmaster's systems, and deprived Ticketmaster of revenue and revenue opportunities.

The defendants moved the district court to dismiss many of Ticketmaster's claims for failure to state a claim, and were

successful in dismissing some of them but the court allowed Ticketmaster leave to amend its complaint. Ticketmaster, 2018 WL 654410, *1 (C.D. Cal. Jan. 31, 2018). However, when defendants moved to dismiss Ticketmaster's amended complaint they were unsuccessful and Ticketmaster's suit stands. Ticketmaster, No. 17-cv-7232, D.I. 48 (C.D. Cal. May 29, 2018).

First, the court upheld Ticketmaster's copyright infringement claim even though it had previously dismissed that claim with leave to amend. In considering defendants' first motion to dismiss, the district court found Ticketmaster's allegations that defendant viewed (and therefore automatically copied) the mobile app and site insufficient to state a claim for copyright infringement. Ticketmaster, 2018 WL 654410 at *3-4. Examining the amended complaint, the district court found that the new allegations regarding defendants' use of bots to download, record, and store Ticketmaster's mobile app content on a hard drive as part of their development of bots was sufficient to state a claim for copyright infringement. Ticketmaster, No. 17-cv-7232, D.I. 48 at 13-14. Interestingly, because Ticketmaster did not have proof of downloading or storing, it relied on an inference that the bot developers must have done so based on the fact that they were very successful at purchasing large amounts of tickets, and that Ticketmaster's mobile app was a complex platform with multiple layers of protection to avoid exactly what the bots accomplished.

The district court also denied defendants' motion to dismiss Ticketmaster's DMCA claim. The court held that Ticketmaster's amended complaint adequately plead this claim because (1) Ticketmaster had copyright protection for its mobile app; and (2) defendants' actions in using bots to avoid the CAPTCHA controls fell within the statute's prohibition against persons "circumvent[ing] a technological measure that effectively controls access to a [copyrighted] work." Ticketmaster, No. 17-cv-7232, D.I. 48 at 22.

The district court also upheld the sufficiency of Ticketmaster's claims under the CFAA and related state statute despite having previously dismissed them. Ticketmaster, No. 17-cv-7232, D.I. 48 at 24-31. The court noted that Ticketmaster's cease and desist letter stated that defendants could not use bots to access Ticketmaster's site. Therefore, Ticketmaster's allegations in the amended complaint that defendants' subsequent use of bots to access the site was unauthorized (even if it did not amount to hacking) was sufficient to state a claim under the CFAA. The court noted that a violation of terms of use, without more, is not sufficient to state a claim under the CFAA. But here, defendants violated the demand in the cease and desist letter, which made their subsequent access to the Ticketmaster site and mobile app unauthorized and exposed them to liability under the CFAA and an analogous state law.

Finally, Ticketmaster's claims for breach of the TOU and fraud withstood defendants' motion to dismiss because defendants agreed to the TOU and then breached it by creating fake accounts and using bots to access the site. Ticketmaster, No. 17-cv-7232, D.I. 48 at 38-29.

This dispute between Ticketmaster and a group of Hamilton-ticket-buying-bot companies highlights the unique issues raised in protecting mobile applications and web content generally. Ticketmaster's copyright protections, coupled with carefully drafted terms of use, and diligent enforcement of its rights may free up a large percentage, and even a majority, of its tickets for purchase by regular customers. Mobile app developers who want to avoid copy-cat apps or data theft, and therefore protect the value of their app, can similarly take steps to protect their content by obtaining patents, trademarks, and copyrights on their work where appropriate. These protections, well drafted terms of service, and other security measures can also lay the foundation for claims under the CFAA and DMCA against competitors who misuse content or access.

* © 2018 Goodwin Procter

This article first appeared in Westlaw's publication entitled Mobile Applications. The publication is part of the Emerging Areas of Practice Series – a new publishing initiative which reduces product to market time to cover emerging areas of the law as they develop. New documents are loaded to Westlaw on a rolling basis as received and content is updated quarterly.

ABOUT THE AUTHORS

Neel Chatterjee (L) is a partner in Goodwin's Intellectual Property Practice. An internationally recognized technology litigator and trial lawyer, Neel has a proven track record of wins in hard-to-win technology cases. His cases often break new ground in undefined areas of the law. Clients frequently turn to Mr. Chatterjee shortly before trial to handle complex technology cases. He is tireless in his efforts to save companies and product lines, as well as to protect core technologies of his clients.

Natasha Daughtrey (R) is an associate in the firm's Litigation Department and a member of its Intellectual Property Group. She joined Goodwin in 2011.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.