AppDetex®
Brand Protection

FIVE REQUIREMENTS FOR CHOOSING A MOBILE APP MANAGEMENT & MONITORING SYSTEM

WHITE PAPER

JULY 2017

FIVE REQUIREMENTS FOR CHOOSING A MOBILE APP MANAGEMENT & MONITORING SYSTEM

Logging into a mobile app store to quickly find and download an app has become as commonplace as picking up a half-gallon of milk at the corner store—in fact, it's even easier and faster. Today's apps promise everything from convenience and efficiency, social sharing, and entertainment to discounts, music streaming, or tools that formerly could only be purchased in the analog world.

With the explosion of smart devices, owners are now awash in (and highly dependent on) mobile apps for their day to day activities. Rogue app publishers have seized the opportunity to leverage the names of some of the most popular trademarks and brands in an effort to increase downloads for their own apps, or worse, to defraud. Unwitting consumers spot something they recognize and with a few clicks, can download and install an app which might turn out to be a completely different app than the one they intended on downloading. To protect against such a problem and potentially lasting damage to their brand, companies must adopt a mobile app management and monitoring strategy.

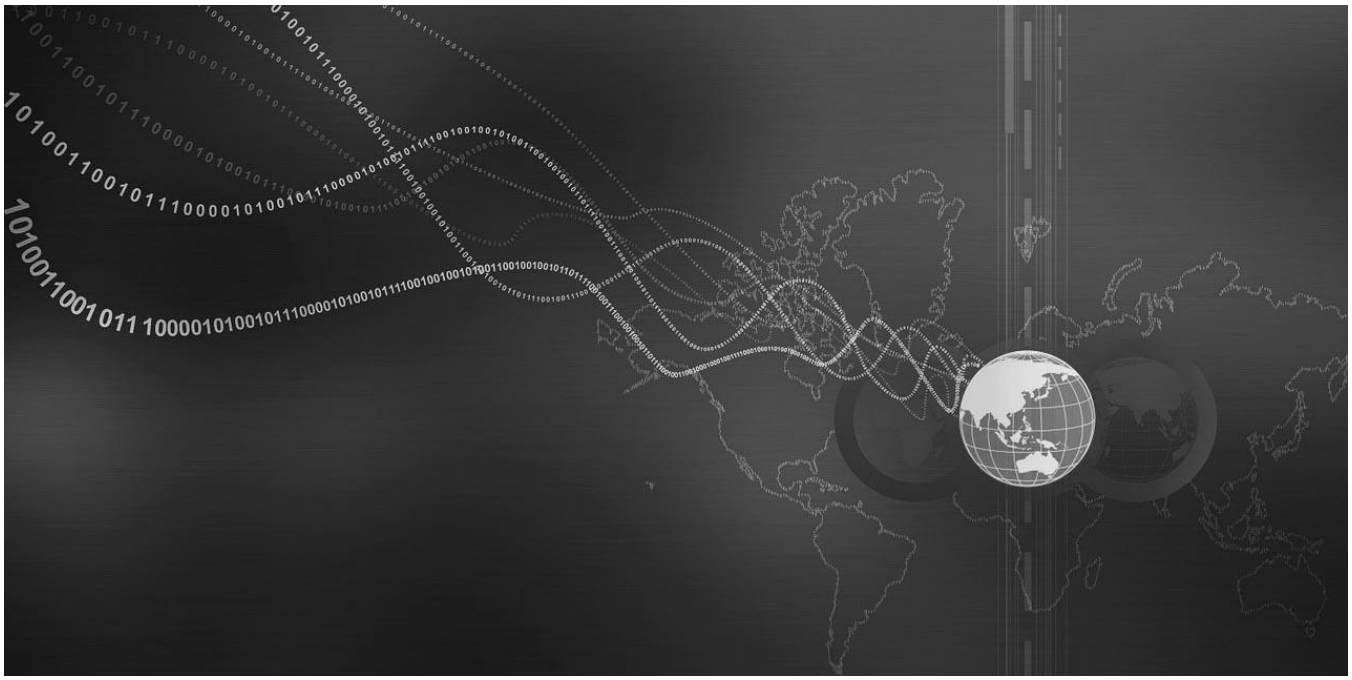
An end to end system that is working efficiently on your behalf should address three key areas: (a) finding relevant and critical data in real time, (b) monitoring potentially infringing apps, and (c) enforcing on apps that are in violation of platform policies or intellectual property. To that end, there are a number of critical functions that should be integrated into a comprehensive mobile app monitoring and management system.

1. INTEGRATED IMAGE RECOGNITION CAPABILITY

Image recognition systems are often confused with more rudimentary image or logo detection systems. The difference is that the former is actually based on image matching while the latter is finding matches based on keywords. Given this obvious shortcoming inherent to detection systems, app publishers will sometimes use proprietary images but omit keywords related to the image to lure consumers into downloading an app, taking advantage of the popularity and recognizable nature of these images. Publishers also understand that tracking images that have no corresponding keywords is difficult for brand holders seeking to enforce their rights. A number of brand protection companies will attempt to describe the two types of monitoring capabilities interchangeably, sometimes in an effort to suggest that they have true image recognition capabilities. Other companies use third-party systems that are not integrated and consequently underperform. It is important, therefore, when shopping for mobile app management and monitoring systems, to be clear as to whether a brand protection company has a) a text-based image detection system, b) its own, internally developed image recognition system, or (c) a third-party system.

2. INTERNATIONAL MONITORING OF MAJOR APP STORES

An effective mobile app management and monitoring system should be able to determine which country an app is published in, particularly in the Google Play and iTunes stores. This can be harder than it sounds given that the app stores only allow you to view apps in the countries associated with your IP address. Thus, if you are located in the US, the stores will display apps associated with US stores. Fortunately, most publishers make their apps available in every store in an effort to increase their download numbers. However, some publishers, recognizing that scrutiny might be less rigorous if your app is displayed in certain other countries, only publish some of their apps in the less trafficked stores.



3. INTERNATIONAL THIRD-PARTY APP STORES

There are a number of new mobile app stores currently in existence across the globe. Many of these stores are in foreign markets (e.g. China and Japan) and largely serve up Android mobile apps for download. It is therefore important for brand holders to first determine which global stores are hosting infringing apps on their site and then prioritize enforcement efforts, starting with the more highly trafficked stores. Although there are a number of app stores that may offer up copycat apps or confusingly similar apps, any foreign store takedown analysis should include a review of which stores have the most traffic, in order to help determine prioritization of enforcement efforts. Without the ability to prioritize, the daunting amount of information that a search potentially yields could be overwhelming, particularly if your brand protection resources are limited.

4. APP LOCK

There are a number of safeguards that should be part of any mobile app monitoring and management system, including approval requirements and duplicate app detection. One critical, and often overlooked, requirement is an internal app lock feature that is designed to guard against the inadvertent takedown of an app by any party using the system. Brand holders often have partners, associated companies, and affiliates they work with on a daily basis. In many instances, these parties are given the right to use the brand holder's intellectual property and brand assets pursuant to certain terms and guidelines. Where the brand holder may have different people working on the app takedown process at any given time, it is critical that the brand holders have a mechanism (an app lock) to prevent legitimate apps from being accidentally removed from mobile app stores.

5. REPORTING

As with any robust system, it is important for a mobile app management and monitoring system to provide detailed reporting metrics that enable the brand holder to track the progress of detection and enforcement activities. These reporting metrics should be generated in real time and should provide enough information relating to store complaints sent; store takedowns (in total and per store); publisher cease-and-desists; publisher changes/takedowns (in total and per store); download diversions averted; and store takedown time (in real time).

ABOUT APPDETEX

Founded in 2012, AppDetex is the global brand protection leader in combatting brand infringement, fraud, and piracy within the increasingly complex worlds of mobile apps, marketplaces, and domains.

We choose to specialize in these three areas, which happen to be the most vulnerable to brand-jacking and, not surprisingly, can be the most difficult to navigate for even experienced IP attorneys. With this focus, we can develop best-in-class technologies and methodologies that expose and enable takedowns of the many egregious and often criminal activities found online today.

Through industry leading innovations in detection and enforcement, AppDetex helps some of the world's most recognizeable brands reduce consumer confusion, brand dilution and fraud while protecting reputations, credibility, and company bottom line.

Led by two experts in the brand protection industry, Faisal Shah and Chris Bura, our company is headquartered in Boise, Idaho.

AppDetex®

Brand Protection

TO LEARN MORE, PLEASE VISIT

WWW.APPDETEX.COM

FOR YOUR OWN BRAND AUDIT / RISK REPORT, PLEASE VISIT

WWW.APPDETEX.COM/FREE-BRAND-AUDIT