LOS ANGELES
Daily Journal
www.dailyjournal.com
THURSDAY, APRIL 17, 2014
PERSPECTIVE

# Mobile app piracy a sign of success?

By Jonathan Blavin

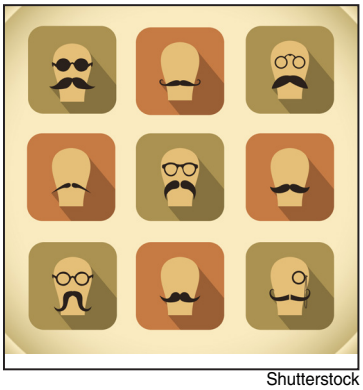
In March, the U.S. government secured its first guilty plea from two individuals accused of distributing copyrighted mobile apps without permission. The individuals sold Android mobile apps through an "alternative online market" to the Google Play store — the site Appbucket — without the permission of the app developers. They reproduced and distributed over a million unauthorized copies of Android mobile apps.

Digital piracy, which has long been the bane of the movie, music and video game industries, now increasingly threatens the mobile app industry, which had approximately $26 billion in sales in 2013. But unlike the traditional large corporate targets of pirates, app developers are not always the Apples and Facebooks of the world, and in many instances are individuals or small companies that do not have the resources to pursue piracy. Apple, Google and others with legitimate app stores have taken certain non-legal measures to protect app developers. In addition to policing its App Store (which also has occasionally been found to contain pirated apps), Apple also works to make its technical security measures thief-proof and to prevent the "jailbreaking" of its iOS software, in which users circumvent various technical protection measures on their iPhones, which, for example, allows them to install unauthorized versions of Apple's App Store that sell pirated apps (such as the infamous, and now shut down, Hackulous/Installous app, which allowed users to transfer easily cracked apps to iOS). In June 2013, Google — whose Google Play Store has at times contained pirated apps and which is less tightly controlled that Apple's App Store — began offering encryption keys with paid apps, which are intended to verify that the app is being used on the same device on which it was purchased and to prevent copying of the app.

Notwithstanding the desire to combat piracy, some app developers have expressed concern that any steps which make it more difficult for users to download and use apps, such as through additional verification steps, will slow sales. Moreover, given the intangible nature of mobile app piracy, it also is challenging for app developers to measure and evaluate whether they are losing sales or attracting interest from early adopters of their apps from the proliferation of unauthorized copies.

As the recent criminal prosecution demonstrates, the law will increasingly play a role in confronting app piracy — though to date has done so with mixed results. Beyond such prosecutions, one area that has received a great deal of attention is the legality of the practice of jailbreaking. Apple, which retains approximately 30 percent of all apps downloaded from its App Store, has a significant interest in curtailing the jailbreaking of its iPhones and other devices. Beyond employing technological barriers to prevent jailbreaking, Apple strongly opposed the librarian of Congress' decision in a triennial rulemaking proceeding in 2010 (reaffirmed in 2013) to exempt from the Digital Millennium Copyright Act's anti-circumvention provisions the jailbreaking of smartphones "to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset." The librarian deemed such modifications made purely for the purpose of software interoperability to be "fair uses." Apple and other copyright owners had emphasized to the office that jailbreaking in the name of interoperability would simply serve as a prerequisite to app piracy. As the Business Software Alliance (of which Apple is a member) argued to the Copyright Office in July 2012, "[j]ailbreaking enables the installation and execution of pirated — i.e., unlicensed — apps on a mobile device .... So there is a direct link between piracy and the circumvention of TPMs [technological protection measures], — jailbreaking is the precondition for making pirated apps valuable."

Although the librarian recognized in his decision the illegality of downloading a pirated app on a jailbroken smartphone device, he concluded that the interests of individual user control over the device trumped such concerns. The librarian relied upon the fact that aside from piracy, the utility of jailbreaking heavily weighs in favor of the advancement of science — e.g., people choose to jailbreak to install interoperable software that can change the aesthetics of the smartphone as well as its functionality, including the appearance of the operating system (such as the keyboard, fonts, backgrounds, etc.), provide additional security measures, such as facial recognition software and enhanced password protection, improve functionality of voice recognition software, and provide the ability to log data usage.


Shutterstock

To be sure, the librarian's decision does not affect those who may traffic in tools used to circumvent technical measures on smartphones, nor does it prevent Apple or other device manufacturers from continuing to employ and improving technical protection measures on their devices. The librarian also declined to extend the jailbreaking exemption to tablet devices in 2013, such as the iPad, as he "found significant merit to the opposition's concerns that this aspect of the proposed class was broad and ill-defined, as a wide range of devices might be considered 'tablets,' notwithstanding the significant distinctions among them in terms of the way they operate, their intended purposes, and the nature of the applications they can accommodate."

Another potential legal avenue in combating piracy is pursuing sites hosting pirated app material. Putting aside those sites located outside the U.S., which are likely beyond the reach of U.S. courts (and which frequently contain unauthorized apps), app stores located in the U.S. are potentially subject to secondary liability for distributing unauthorized versions of copyrighted apps if they do not comply with the DMCA's notice-and-takedown provisions. Courts, however, generally have construed the DMCA's safe harbors to place the burden almost entirely on copyright owners to identify and seek the removal of infringing works, creating a whack-a-mole problem. Although courts generally have held that the DMCA does not impose on service providers a duty to monitor their sites for infringing materials, courts also have stressed that a provider cannot willfully blind itself to blatant infringement and nonetheless claim a lack of knowledge of infringement. For example, the 7th U.S. Circuit Court of Appeals in *In re Aimster Litigation*, 334 F.3d 643, 650-51 (7th Cir. 2003), held that a service provider cannot encrypt the users' data so as to intentionally keep itself unaware of the identity of infringers. The 2nd Circuit in *Viacom Intl. Inc. v. YouTube Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) also confirmed that the DMCA "limits — but does not abrogate — the doctrine" of willful blindness.

Infringement on legitimate app stores raises interesting questions regarding the doctrine of willful blindness. For example, in 2011, the Apple App Store contained a game called "Lugaru HD," by Wolfire Games, and a game called "Lugaru," by iCoder. They were, in fact, the exact same game, the only difference being the price, with the unauthorized copy being sold for $8 less than the original. Like others, however, Apple's App Store requires a period of review before a work will be made available for sale; every submission to Apple's App Store is said to be reviewed by two people, and the process averages about two weeks. For Amazon's Kindle Store, works are available approximately 24 to 48 hours after submission and appear to be checked only by an automated computer process. Whether app stores can hide behind automated review processes to insulate themselves from liability under the DMCA has yet to be determined, though courts generally in other instances have held that the existence of any kind of review and approval process establishes knowledge and renders the service provider outside of the DMCA's safe harbors.

As the app economy continues to grow, app piracy likely will increase in equal measure. Whether the law will be able to confront such piracy effectively remains an open issue.


JONATHAN BLAVIN
*Munger, Tolles & Olson*

**Jonathan Blavin** *is a partner at Munger, Tolles & Olson LLP. He can be reached at Jonathan.Blavin@mto.com.*