



March Madness or April Fools?

A Mobile App Risk Assessment Report by

FLEXERA[®]
SOFTWARE

Contents

Introduction.....	3
Test Result Highlights.....	5
Test Results in Detail.....	6
Test Descriptions.....	6
Infographic.....	10
About Flexera Software.....	11

March Madness or April Fools?

A Mobile App Risk Assessment Report by Flexera Software

Introduction

It's March Madness, and as the hearts and minds of basketball-loving Americans turn to office pools, brackets, and the Final Four – the workplace is crowded with employees checking their mobile apps for the latest scores to see how their teams are advancing.

It's no secret that March Madness has impacts in the workplace. According to a 2015 [report](#), an estimated 50 million American employees participate in March Madness office pools; 9.9 million stream March Madness coverage, and 56% plan to spend at least one hour of their workday on March Madness activities. And employers rack up as much as \$1.25B in lost wages due to employee March Madness distractions.

And mobile devices and mobile apps make it easier than ever for employees to get their March Madness fix. Here are a few of the popular ones:

- **March Madness Live** is an app platform which allows users to watch all 2016 NCAA (Men's College Basketball Tournament) games on during the tournament.
- **Yahoo! Sports** allows users to create and participate in March Madness 2016 NCAA brackets with their "Tourney Pick 'Em" site available, which keeps track of scores throughout the tournament and provides ease of use for switching between sports and games.
- **ESPN Tournament Challenge** is a bracket app for the NCAA Men's College Basketball Tournament. Users can start a group, invite friends, make bracket picks, and compete against politicians, professional athletes, favorite stars, and ESPN talent.
- **CBS Sports** app lets fans create, manage and socialize their college basketball brackets, watch NCAA basketball games live and get the latest scores, stats and news.

With the proliferation of corporate-issued mobile devices and employees accessing corporate data from their personal devices (via corporate Bring Your Own Device [BYOD] policies) – is there another March Madness downside for organizations beyond employee distraction?

What about the apps employees are using on their corporate and BYOD devices to stream content, complete brackets and track March Madness activities? What data can they access? What device features can they interact with? Could they pose a potential security risk to organizations or violate their BYOD policies?

CIO's are very good about keeping track of the myriad enterprise applications running on their networks, understanding what those applications do and mitigating risks. Indeed many leading enterprises have centralized [Application Readiness](#) processes to test applications and understand their behavior before they go live. However few organizations extend those processes to mobile apps. According to a recent Flexera Software [report](#), 61 percent of organizations haven't identified which mobile app behaviors they would deem risky. And 55 percent haven't identified which mobile apps they'd deem risky.

This begs the question – is a corporate CIO putting her organization at risk and her reputation in jeopardy by failing to understand the behaviors of mobile apps employees are using that interact with corporate systems and data? In other words, could March Madness apps make the CIO an April Fool?

We examined 28 popular media and sporting apps that are available in the Apple App Store to assess them for potential BYOD risk to organizations, including:

Breaking!	MarchMadnessLive	Thuuz
CBS Sports	Rotoworld	TournamentChallenge
Daily Bracket	SeatGeek	TuneIn Radio
DIRECTV	Yahoo Sportacular	Twitter
DISH	Sports Feed	Watch TBS
DraftKings	Sportsmanias	Watch TNT
ESPN	StubHub	WatchESPN
fanatic	SXMLiveAudioPlayer	XPlay
FanDuel	Team Stream	
FantasyFootball	theScore	

We ran tests on these apps using [Flexera Software's AdminStudio Mobile](#) which helps organizations identify, manage, track and report on mobile apps, simplify mobile application management, reduce mobile app risk and address the rapidly growing demand for mobile apps in the enterprise.

AdminStudio Mobile tested these apps to determine whether they interact with an Apple iOS device's:

- Ad Network
- Address Book
- Bluetooth
- Calendar
- In-app Purchasing
- Location Services
- Sharing
- Functionality
- SMS/Texting
- Social Networking
- Telephony

A description of what the test results mean and their potential risks to the enterprise can be found in the [Test Descriptions](#) section of this report. There are many dating apps not tested in this report that are available in public app stores and that employees could download to their corporate-issued or BYOD phones. The results highlighted in today's report simply underscores the importance of knowing what those apps do and how they could interact with sensitive corporate data.

Test Result Highlights

Of the 28 popular Apple iOS apps tested:

- 89 percent, including Daily Bracket, ESPN and March Madness Live, support Ad Networks.
- 79 percent, including CBS Sports, Dish and Tournament Challenge are capable of accessing the device's location tracking functionality.
- 71 percent, including CBS Sports, Daily Bracket and March Madness Live are capable of accessing and sharing data with social networking sites connected to the device.
- 68 percent, including ESPN, Sports Feed and Twitter can access the device's SMS texting functionality.
- 61 percent, including CBS Sports, ESPN and March Madness Live can access the device's calendar.

Test Results in Detail



Mobile App	Ad networks	Address book access	Bluetooth LE	Calendar access	In-app purchasing	Location services	Location tracking	Share	SMS	Social networking	Telephony
Breaking!	✓	○	○	✓	✓	○	✓	○	○	✓	✓
CBS Sports	✓	○	✓	✓	✓	○	✓	○	✓	✓	✓
Daily Bracket	✓	○	○	○	✓	○	✓	○	✓	✓	✓
DIRECTV	○	○	○	○	○	○	○	○	○	○	○
DISH	✓	○	○	✓	○	○	✓	○	✓	✓	✓
DraftKings	✓	○	✓	○	✓	○	✓	○	✓	○	✓
ESPN	✓	✓	○	✓	✓	○	✓	○	✓	✓	✓
fanatic	✓	○	○	○	○	○	✓	○	○	✓	✓
FanDuel	✓	○	✓	○	○	✓	✓	○	✓	✓	✓
FantasyFootball	○	○	○	○	○	✓	○	○	○	○	○
MarchMadnessLive	✓	○	○	✓	○	○	✓	○	✓	✓	✓
Rotoworld	✓	○	○	✓	✓	○	✓	○	✓	○	✓
SeatGeek	✓	✓	○	✓	○	○	✓	○	✓	✓	✓
Yahoo Sportacular	○	○	○	○	○	○	○	○	○	○	○
Sports Feed	✓	✓	○	✓	✓	○	✓	○	✓	✓	✓
Sportsmanias	✓	○	○	○	✓	○	✓	○	✓	✓	✓
StubHub	✓	✓	✓	✓	✓	○	✓	○	✓	✓	✓
SXMLiveAudioPlayer	✓	○	○	○	✓	○	✓	○	○	✓	✓
Team Stream	✓	○	○	✓	✓	○	○	○	✓	✓	✓
theScore	✓	○	○	✓	✓	○	✓	○	○	✓	✓
Thuuz	✓	○	○	○	✓	○	✓	○	✓	✓	✓
TournamentChallenge	✓	○	○	✓	✓	○	✓	○	✓	✓	✓
TuneIn Radio	✓	✓	✓	✓	✓	○	✓	○	✓	✓	✓
Twitter	✓	✓	○	○	✓	✓	✓	✓	✓	○	✓
Watch TBS	✓	○	○	✓	✓	✓	✓	○	✓	✓	✓
Watch TNT	✓	○	○	✓	✓	✓	✓	○	✓	○	✓
WatchESPN	✓	○	○	✓	✓	○	○	○	○	○	✓
XPIag	✓	○	○	✓	✓	○	○	○	○	○	✓
Total Percentage	89%	21%	18%	61%	71%	18%	79%	4%	68%	71%	89%



iOS Feature Use

This report lists the usage/requirement status of the selected iOS feature(s) for all iOS apps in the Application Catalog. To change the selected feature, or to select multiple features, click **Options** in the toolbar.

Legend

- Uses feature 
- Does not use this feature 

Test Descriptions

Flexera Software AdminStudio Test: **Ad Network**

- **What does this test result mean?** The app is capable of displaying advertisements “in-app” and connecting to ad networks
- **Potential risk to enterprises:** Online ads frequently come from ad networks that supply code that developers use to insert advertisements into their apps. These ad networks could be vulnerable to hacking, thereby exposing the device and its data to illegal access by a malicious third party.

Flexera Software AdminStudio Test: **Address Book Access**

- **What does this test result mean?** The app is able to access the device’s address book.
- **Potential risk to enterprises:** Address books are important to advertisers. If an app is capable of addressing the device’s address book, that data could be used by the app developer or shared with third parties such as advertisers, which may violate an organization’s privacy, confidentiality or BYOD policies.

Flexera Software AdminStudio Test: **Bluetooth LE**

- **What does this test result mean?** The app is capable of accessing the device’s Bluetooth phone features
- **Potential risk to enterprises:** Hackers with specific intent can potentially gain access to data being communicated by the device via Bluetooth communications. If the app in question is capable of accessing private, confidential or sensitive data on the device – and that device’s Bluetooth data has been hacked, this could cause a security risk for an organization.

Flexera Software AdminStudio Test: **Calendar Access**

- **What does this test result mean?** The app is capable of accessing the device’s calendar and calendar functions
- **Potential risk to enterprises:** Similar to risks associated with apps that access the address book, data from a user’s device calendar could be accessed and used by the app developer or shared with third parties, such as advertisers. Given the private, confidential and/or sensitive nature of calendar content – giving apps access to this data may create unwanted security risk depending on the organization and its BYOD policies.

Flexera Software AdminStudio Test: **In-App Purchasing**

- **What does this test result mean?** The App enables in-app purchasing
- **Potential risk to enterprises:** In-app purchasing capabilities could expose an organization to unwanted additional costs if the device is tied to a corporate credit card account. An organization might have other software licensing and compliance policies around app procurement that could also be circumvented by in-app purchasing.

Flexera Software AdminStudio Test: **Location Services**

- **What does this test result mean?** The app can access the device's GPS location services
- **Potential risk to enterprises:** Confidentiality and privacy concerns in many organizations would prohibit unapproved apps from tracking employee location information. Moreover, to advertisers, location is one of the most valuable things on a device, so many apps access this data solely to pass along to advertisers. Consequently many organizations restrict apps that can access location services on employer-issued or BYOD devices.

Flexera Software AdminStudio Test: **Sharing Functionality**

- **What does this test result mean?** The app is able to access the device's share feature
- **Potential risk to enterprises:** The device's share feature gives users a convenient way to share content with other entities, such as social sharing websites or upload services. Employer-issued and BYOD devices may be linked to corporate social media and other accounts. If the share function on the device is accessed, personal employee data or content could inadvertently be shared to a corporate social media site. Some companies may have policies against allowing apps onto employer-issued or BYOD devices capable of accessing the share function.

Flexera Software AdminStudio Test: **SMS/Texting**

- **What does this test result mean?** The app can access the device's text functionality
- **Potential risk to enterprises:** Apps that can access the device's SMS functionality can potentially read text messages that are stored on the phone, or create text messages and send them to recipients – for instance contacts on the device (if the app can also access the contact list). This poses significant potential privacy concerns for corporate-issued or BYOD devices, given that confidential information could be contained in the text messages.

Flexera Software AdminStudio Test: **Social networking**

- **What does this test result mean?** The app can access and share data with social networking sites
- **Potential risk to enterprises:** Employer-issued and BYOD devices often contain confidential information that should not be shared in a social media setting. Apps able to access social media sites could potentially share confidential data. Likewise, a

corporate or BYOD device that contains personal employee content could inadvertently share personal data to a corporate social media site linked to the device.

Flexera Software AdminStudio Test: **Telephony**

- **What does this test result mean?** The app can access the devices phone function
- **Potential risk to enterprises:** There is a risk that an app accessing telephony features could call restricted phone numbers or “premium” phone numbers that, for instance charge high fees – such as per-minute calling charges. In some instances, organizations may want to restrict apps capable of accessing a device’s telephony function.

Infographic



About Flexera Software

Flexera Software helps application producers and enterprises increase application usage and security, enhancing the value they derive from their software. Our software licensing, compliance, cybersecurity and installation solutions are essential to ensure continuous licensing compliance, optimized software investments, and to future-proof businesses against the risks and costs of constantly changing technology. A marketplace leader for more than 25 years, 80,000+ customers turn to Flexera Software as a trusted and neutral source of knowledge and expertise, and for the automation and intelligence designed into our products. For more information, please go to: www.flexerasoftware.com.



www.FlexeraSoftware.com