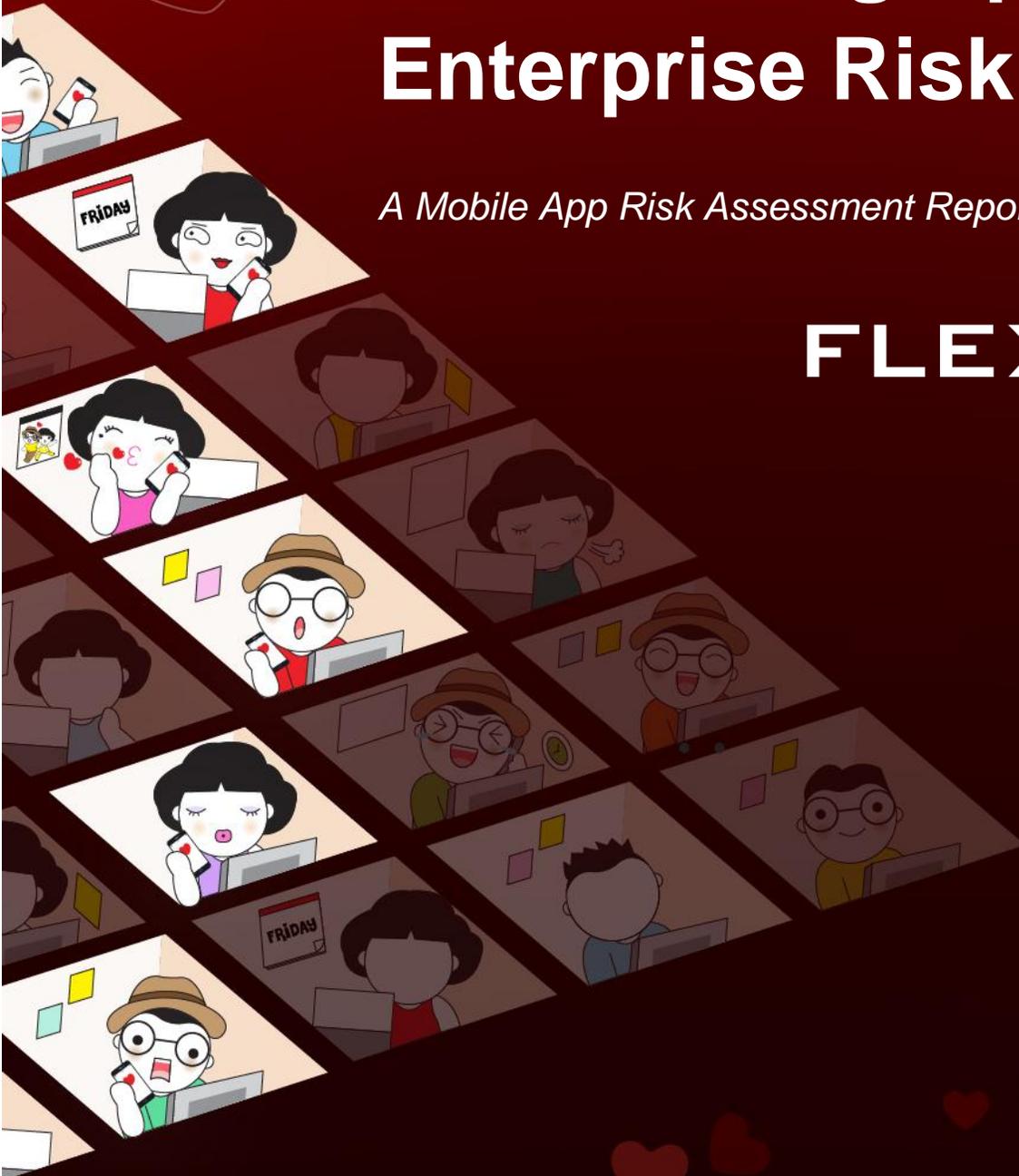


Bring Your Own Date: Love, Dating Apps & Enterprise Risk

A Mobile App Risk Assessment Report by

FLEXERA[®]
SOFTWARE



Contents

Introduction.....	3
Love and the Single Employee: Dating Apps and 'Bring Your Own Date' (BYOD)	4
Test Result Highlights.....	5
Test Results in Detail.....	6
Test Descriptions.....	7
Infographic	10
About Flexera Software.....	11

Bring Your Own Date: Love, Dating Apps & Enterprise Risk

A Mobile App Risk Assessment Report by Flexera Software

Introduction

Mobile devices are almost ubiquitously used by employees today. Whether companies issue corporate-owned devices, or whether they allow employees to access corporate networks via their own devices (Bring your Own Device) – employees can easily access corporate networks and sensitive enterprise data with a flick or a swipe.

As mobile devices make it easy for us to access our entire lives at a glance, the dividing line between professional and personal is getting fainter. Employees commonly install personal apps on devices they also use for work. And most don't think twice about whether an app they're using could potentially expose the corporate network to risk.

It is therefore incumbent on the Chief Information Officer and Chief Security Officer to understand what the mobile apps on employee devices can do – what data, features and functions they can access – and determine whether this behavior is acceptable based on the organization's Bring Your Own Device policy. Testing mobile apps to discover their behavior and risks should be part of any organization's centralized [Application Readiness](#) processes.

Love and the Single Employee: Dating Apps and ‘Bring Your Own Date’ (BYOD)

As Valentine’s Day approaches, employees are busy finalizing their plans for romance. Whether it’s making reservations at a favorite local restaurant, ordering flowers and chocolates, or simply planning a special evening at home – love is in the air.

For employees that don’t have a significant other to share Valentine’s Day with – no worries. A healthy supply of dating apps are available for download – making it easy for them to swipe their way to romance in time for February 14. Given the popularity of dating apps for today’s high-tech singles, we examined 25 popular dating apps available in the Apple App Store to assess them for potential BYOD risk to organizations, including:

- Blendr
- Bumble
- Coffee Meets Bagel
- E-darling
- Gleeden
- Grindr
- Happn
- Hinge
- Hitch
- HowAboutWe
- Lovestruck
- LOVOO
- Match
- MySingleFriend
- NeuChat
- OKCupid
- Once
- Parship
- POF
- RSVP
- Sexy Flirt
- Single.de
- Tastebuds
- Tinder
- Zoosk

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
- Camera
- 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 on popular dating

apps simply underscores the importance of knowing what those apps do and how they could interact with sensitive corporate data.

Test Result Highlights

Of the 25 popular Apple iOS dating apps tested:

- 88 percent of the apps tested, including Grindr, OKCupid and Tinder, are capable of accessing a device's location services.
- 76 percent of the apps tested, including Blendr, HowAboutWe and Zoosk support ad networks.
- 60 percent of the apps tested are capable of accessing the device's social networking apps as well as SMS/Texting functions
- 36 percent of the apps tested, including Grindr, Lovestruck and OKCupid are capable of accessing the device's calendar.
- 24 percent of the apps tested, including Blendr, Hinge and Tinder are capable of accessing the device's address book.

Test Results in Detail

Mobile App	Ad networks	Address book access	Bluetooth LE	Calendar access	In-app purchasing	Location tracking	Share	SMS	Social networking	Telephony
Blendr	✓	✓	○	○	○	✓	○	✓	✓	✓
Bumble	✓	○	○	○	✓	✓	○	✓	✓	✓
Coffee Meets Bagel	✓	✓	○	✓	✓	✓	○	✓	✓	✓
E-darling	✓	○	○	○	✓	○	○	○	○	✓
Gleeden	○	○	○	○	✓	✓	○	○	○	○
Grindr	✓	○	○	✓	✓	✓	○	○	○	✓
happn	✓	○	○	○	✓	✓	○	✓	✓	✓
Hinge	✓	✓	✓	○	○	✓	○	○	✓	✓
Hitch	○	○	○	○	✓	✓	○	✓	○	✓
HowAboutWe	✓	✓	○	○	✓	✓	○	○	○	✓
Lovestruck	✓	○	○	✓	○	✓	○	○	✓	○
LOVOO	✓	○	○	✓	✓	✓	○	✓	✓	✓
Match	○	○	○	○	○	○	✓	○	○	○
MySingleFriend	✓	○	○	○	✓	✓	○	✓	✓	✓
Neu Chat	○	✓	○	○	✓	✓	○	○	○	○
OkCupid	✓	○	○	✓	✓	✓	○	✓	✓	✓
once	✓	○	✓	○	✓	✓	○	✓	✓	✓
Parship	○	○	○	○	○	○	○	○	○	○
Plenty of Fish	✓	○	○	✓	✓	✓	○	✓	✓	✓
RSVP	✓	○	○	✓	✓	✓	○	✓	○	✓
Sexy Flirt	✓	○	○	○	✓	✓	○	✓	✓	✓
single.de	✓	○	○	✓	✓	✓	○	✓	✓	✓
Tastebuds	○	○	○	○	○	✓	○	○	○	○
Tinder	✓	✓	○	○	✓	✓	○	✓	✓	✓
Zoosk	✓	○	○	✓	✓	✓	○	✓	✓	✓
Total %	76%	24%	8%	36%	76%	88%	4%	60%	60%	76%



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.

BRING YOUR OWN DATE:

Love, Dating Apps
& Enterprise Risk



OF THE **25**
POPULAR APPLE IOS
DATING APPS TESTED:

88%

including Grindr, OKCupid and Tinder, are capable of accessing a device's location services.

76%

including Blendr, HowAboutWe and Zoosk support ad networks.

60%

are capable of accessing the device's social networking apps as well as SMS/Texting functions

36%

including Grindr, Lovestruck and OKCupid are capable of accessing the device's calendar

24%

including Blendr, Hinge and Tinder are capable of accessing the device's address book.



A Mobile App Risk Assessment Report by



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