airwatch by vmware

Demystifying End-user Privacy for Enterprise Mobility

Tangible actions to secure your mobile fleet and put Privacy First.

Table of Contents

INTRODUCTION

Technology—particularly mobile technology, such as smartphones and tablet PCs—has fundamentally changed the way organizations around the globe do business. With the U.S. mobile workforce projected to reach over 105 million employees by 2020, mobility has transformed the way modern work gets done inside and outside of the traditional office environment.[1]

With this transformation, however, new challenges and threats arise for modern global businesses, from mobile availability of business-critical assets to privacy and security concerns.

91%

of surveyed users said they have lost control over how companies access and use their personal information.[2]

86%

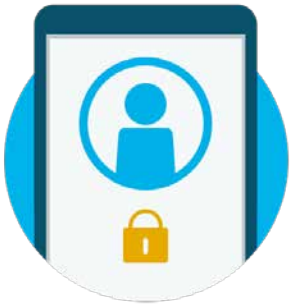
tried to remove or mask their online digital footprint.[2]

Many companies today are offering "bring-your-own" programs to employees, giving them access to corporate applications and data on their personal devices, while maintaining a level of enterprise security on the device. As a result, end users are becoming increasingly concerned with how their personal information and actions may be exposed to their employer. Employees are often confused and misinformed about the types of information employers can access on their personal devices, and this disconnect can cause deep-seated distrust throughout the organization.

While an enterprise mobility management (EMM) solution like AirWatch is the most simple and scalable way to make business data and applications available on mobile devices, today's modern enterprise faces a monumental challenge that could make or break the success of a workforce mobility program: end-user privacy.

Delivering end-user privacy is more than an ideal practice; in many cases, user privacy is both a legal requirement and a necessity for business mobility adoption and success. Organizations that operate globally are also challenged to comply with local laws and regulations as it relates to end-user privacy and data transfer. Enterprises must comply with in-country privacy and data localization regulations, most of which vary widely in legal scope and requirements from region to region and country to country. What works for information management in the United States does not necessarily work in Germany. Employees also must trust both the organization and the solution to allow access to their devices and grant management permission. These two influencers have the potential to pose significant threats to the company's operational success.

Establishing both the right solution and the right privacy components is crucial for businesses transformation through enterprise mobility. To gain end-user trust, secure enterprise data and attain regulatory compliance, AirWatch puts user privacy first.



AIRWATCH PRIVACY FIRST

With these two monumental challenges facing today's modern enterprise, establishing end-user trust in EMM solutions is crucial for success.

AirWatch's longstanding dedication to privacy has continued to evolve with every iteration of its products, with a focused intensity on better protecting end users and providing governance for organizations. AirWatch formalized this dedication with the introduction of its **Privacy First Program** in 2015. Built on Fair Information Practice Principles, the program is founded on two themes: helping organizations comply with privacy principles by offering privacy controls and providing transparency and choice to employees.

105 MILLION

size of the U.S. mobile workforce by 2020.[1]

Empowering Organizations with Privacy Controls

AirWatch is focused on providing built-in controls, configuration options, and features to help organizations comply with their unique organizational and regulatory privacy requirements.

IT Admin AirWatch Privacy First capabilities include:

Data Transfer

» **Multitenant privacy settings for data collection and display:** Includes the ability to turn off personal app and GPS collection, as well as factory wipe prevention only for BYOD. This allows for granular control over what an admin collects from their device and user population.

» **Role-based access:** Admin Roles within the AirWatch Admin Console allows you to define various access levels based on corporate groups or individual users. AirWatch recommends that administrators have the minimum amount of access required to perform their job duties.

Carefully consideration should be taken when creating roles to ensure personal information is not accidentally exposed to an admin that does not require it to do their job.

» **Data encryption of personally identifiable information:** User-specific information will be encrypted at the database level. This provides additional security in the event of a data breach, as lost/stolen data that is encrypted is not considered a threat unless the encryption key is also compromised.

Data Access

» **Remote file storage:** Enables Secure Content Locker to use a remote repository to retrieve corporate materials and comply with strict data transfer laws such as those in Germany and Russia, where personal citizen data cannot leave the country by law. Secure Content Locker can be configured to use the remote repository to retrieve documents and other corporate materials without physically moving the file into an unapproved location.

» **Anonymized API scan:** App Scan allows the administrator to send a list of applications that are installed on the device fleet to a partnered list of app scan vendors. They then analyze the list and look for applications that have been known to contain malicious or harmful code before reporting back to AirWatch with the results. Administrators can then create an application blacklist, along with compliance policies that take action on devices containing that application. The APIs for this functionality automatically remove all personally identifiable information and only send an aggregated list of applications to the App Scan vendors. By using this method, administrators are not subject to data transfer laws, as the de-identified information transferred is not considered personal.

Native vs. Proprietary Containerization

Proprietary containerization is technology provided by EMM providers, such as AirWatch, and third-party vendors to enable Mobile Application Management (MAM) and containerized data on end-user devices. Proprietary protocols and APIs must be used to deploy containerization.

Native containerization builds MAM and containerization capabilities into the native operating system, made possible by recent innovations in iOS, Android and Windows mobile operating systems.

End User AirWatch Privacy First capabilities include:

Education and Transparency for End Users

» **Custom enrollment email:** Before an end user begins the enrollment process, they can automatically receive a "device activation" email from AirWatch. The HTML-ready customizable templates allow IT admins to provide enrollment instructions along with what they can expect from

their enrollment experience. This is a great tool to inform end users of the privacy implications of enrollment and call out those areas that will not or cannot be monitored, such as personal apps and email, text messages, photos/videos, GPS and phone records.

» **Custom privacy notice: Customizable, HTML-ready notices can be configured using an AirWatch message template and displayed to end users as they enroll or begin using a new application. This is a great way to educate users on potential areas of concern, such as the collection of personal applications and GPS, as well the lack of the organization's ability to read personal email, text, photos/videos and phone records.**

» **Self-service portal:** The self-service portal is a tool that provides transparency between IT admin and end user. If granted "full access" (AW best practice), end users will have the same access to their device information and actions as the IT admin. This same console includes device details, compliance status, and historical application lists. Actions such as device lock, un-enroll, password reset and device wipe are also available for self-sufficient troubleshooting.

Containerization & Privacy

The most sought-after BYOD enablement functionality is the ability to compartmentalize work and personal data on employee-owned devices. This contained separation ensures that IT can access and manage only work-related apps and settings, safeguarding end-user privacy by making personal apps and data inaccessible. The notion of separating work and personal data can be referred to as containerization.

Regardless of the container approach deployed by enterprises, privacy will be a perceived issue for end users—but in different ways. With native containers, the user is trusting the operating system and sees familiar consumer brand names and native prompts to consent to disclose their personal information—just like they would in any other app. With proprietary containers, the user is trusting custom software that can operate a bit like a black box—not necessarily built on the OS' trust framework and may be inadvertently collecting personal information.

Providing Transparency & Choice to Employees

AirWatch sells to IT administrators who fully understand the limitations of the software's data collection. However, AirWatch is installed directly onto employee devices. While IT understands what can and cannot be tracked on a device and mobile operating systems make it impossible for EMM providers to read data in certain mobile applications, such as text messaging, employees often think of the software as "big brother." This misconception and the lack of transparency provided by operating systems can damage user adoption and hinder organizational transformation through business mobility.

Within the mobile architecture, there are two basic ways consent is given:

1. During device enrollment in EMM, MAM and/or MDM
2. Within the application upon download or first-time access

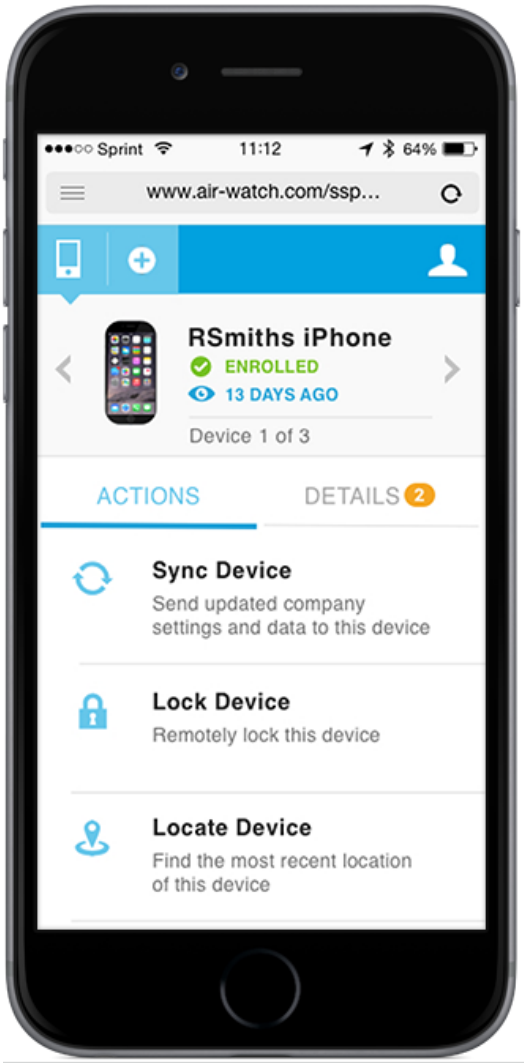
Architecturally, certain device functionalities are impossible to collect, including user photos, text message contents and personal email.

A major barrier to adoption is simply education, helping end users understand what can and cannot be tracked on their mobile devices. To empower this vital component, AirWatch aims to proactively provide IT managers with the tools they need to educate their employees on user privacy and provide the transparency needed to establish organizational trust in BYO programs.

AirWatch is dedicated to providing transparency, access and choice to end users by:

» Providing full visibility and access to personal information via the AirWatch Self Service Portal app that can be enabled by the IT administrator and distributed to end-user devices automatically

» Displaying personal information being collected in a user-friendly HTML format during enrollment



» Notifying users of policy changes as they are implemented

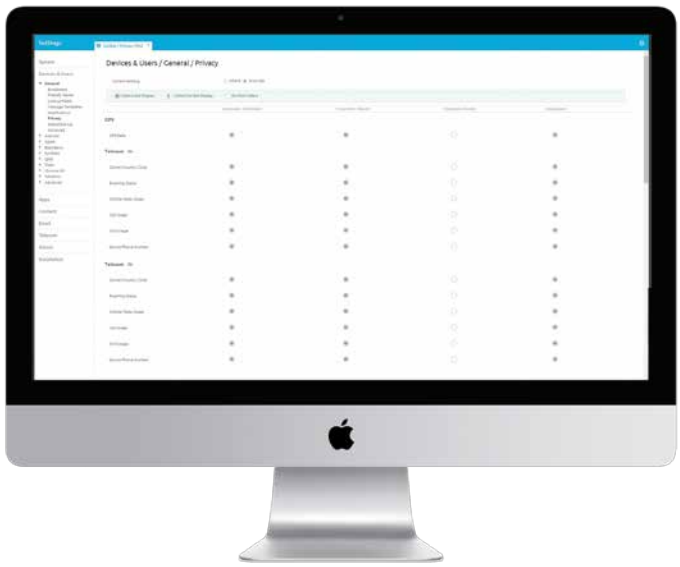
» Sending users additional, granular privacy notices for each app download

» Giving users complete control with the ability to delete data or opt out of the service

» Honoring the native built-in operating system privacy framework and consent notices, such as the notice on devices that users must affirmatively opt into for GPS location collection

AIRWATCH BEST PRACTICES FOR BYOD PRIVACY

AirWatch recommends setting each area of personal information collection to “Do Not Collect” for employee-owned devices unless there is a specific use case where it must be enabled.



AirWatch’s recommendation is to set all of these values to “prevent” unless there is a specific use case where it must be enabled. Having permission to “full wipe,” or factory reset, a BYOD device may lead to accidental removal of personal text, photos, videos and content from an end user’s device. Although it may provide benefit to the end user if their device is lost or stolen, it is important to weigh the pros

AirWatch recommends that organizations create a distinct privacy notice for its BYOD devices, separate from corporate-owned policies. If different privacy settings impact specific platforms (i.e. iOS vs. Android), organize the groupings by using the “platforms” option. The privacy notice should ensure that the employee understands:

» The areas where their personal information will be collected

» Who they can contact to gain access to that information and make corrections where applicable

» That they can halt the enrollment process now by exiting the agent if they are uncomfortable with the collected information

» The benefits they will receive upon completing enrollment

Those four key areas should be called out in a simple and easy-to-understand fashion to increase the likelihood that an end user reads and understands the privacy policy.

The Self Service Portal is a great way to empower self-sufficiency and provide transparency between IT administrators and end users. AirWatch recommends granting BYOD end users "full access" to the Self Service Portal to help them understand the level of IT access to their device. Information available includes device details, compliance status and historical application lists. Actions such as device lock, un-enroll, password reset and device wipe are also available for self-sufficient troubleshooting and end-user device management.

CONCLUSION

The balancing act of enterprise data security and end-user privacy is one of the top concerns for today's increasingly mobile businesses. On one hand, empowering workforce mobility with enterprise apps is proven to increase worker productivity by nearly 40% and consequently drive business growth.[3] On the other hand, as business-critical data moves outside the physical and virtual walls of the enterprise, the risk for corporate data vulnerability increases exponentially. Surrounding both is the ever-present concern about end-user privacy, particularly in BYOD environments.

The AirWatch Privacy First initiative was developed to help IT teams transform business mobility management from a balancing act to a mobile strategy purpose-built to educate and empower productivity, security, innovation and growth.

Security & Privacy Controls for Enterprises

- Multitenant privacy settings for data collection and display
- Role-based access
- Database encryption of personally identifiable information
- Remote file storage
- Anonymized app scan APIs

Transparency & Privacy for End Users

- Custom privacy notice per app and for program enrollment
- Custom enrollment email for education
- Self Service Portal

Learn More

Join the conversation on Twitter

Start Free AirWatch Trial

Additional Resources

For additional information, visit the AirWatch Blog:
blogs.air-watch.com/

1. https://www.idc.com/getdoc.jsp?containerId=prUS25705415
2. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/
3. https://hbr.org/2014/11/the-productivity-payoff-of-mobile-apps-at-work

AirWatch Global Headquarters

1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch by VMware

AirWatch by VMware is the leader in enterprise mobility management, with more than 14,000 global customers. The AirWatch platform includes industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at **www.air-watch.com**.