WHITE PAPER

MOBILE DATA PRIVACY

Risk analysis, Legal framework & Breach prevention

pradeo

INDEX

INTRODUCTION

Mobile services are increasingly being used for daily activities, for both personal and professional purposes, and being accessed from devices that cannot always be trusted. These usages imply billions of corporate data constantly transiting between information systems, applications and endpoints, widening existing perimeters. At the same time, authorities, customers and collaborators are expecting organizations to fully ensure the privacy of the data handled through mobile, by deploying the appropriate means to prevent breach.

This white paper gathers the key elements security heads should know to successfully address mobile data privacy within their global strategy.

THE BOOMING OF MOBILITY

89% of employees use their smartphone or tablet for work

82% of internet users in the US use their mobile device to shop online

4h are spent everyday by users on their smartphone

70% of mobile time is spent on applications

Enterprise mobility

According to a Gartner survey and to Mikako Kitagawa, principal research analyst at Gartner, nearly 80% of employees say they haven't received employer-issued smartphones and more than 50% of employees exclusively use their personal mobile device in the workplace (BYOD).

Organizations are more and more flexible regarding their employee's working tools and locations. As a result, they often access business data and applications from home, coffee shops or airports using their mobile device, by connecting to public networks.

Enterprise mobility has led to the obsolescence of standard security solutions historically used by companies (ie: antivirus), as they don't cover the perimeter of mobile devices and applications.

Mobile applications

Digitalization impacts users' behavior by creating and meeting a need of immediacy. People are in constant demand for agility and flexibility, and mobile applications have become the main answer to this need. In 2021, mobile users were spending 70% of their time in applications, according to Frost & Sullivan.

Daily tasks such as emailing, banking, fitness tracking, shopping, etc. are nowadays mostly done using mobile applications. As a result, they manipulate critical data (credentials, banking details, geolocation, pictures, SMS…) and have the possibility to exfiltrate those information, relying on the permissions they are given.

RISK EVALUATION

Step 1 - Data mapping

Mobility is vast and results in numerous data exchanges, making mobile frameworks sometimes difficult to visualize. The data mapping below represents all the flows potentially created by the usage of mobile devices and applications. As a first step, organizations that leverage mobility to enhance their operations must define which parts of this mapping apply to their structure and list where data are sent and stored.

Pradeo's mobile security solution suite provides audit tools to:

- Identify the data manipulated by the mobile devices within a fleet
- Reveal all the data processed and exfiltrated by mobile applications

Step 2 - Data sensitivity

Once the mobile framework and all the data flows are clearly defined, all the data handled need to be qualified. Information that are valuable to the company as well as the one that fall under dedicated legislations need to be identified and tracked. For example, as personal data processing is strongly regulated by some laws like the General Data Protection Regulation, they require organizations to pay them a special attention.

Step 3 - Data exposure

After having carried out the first two steps, security heads will be able to determine whether sensitive and valuable data are manipulated through their mobile framework and what's their degree of exposure to attack and leakage. Eventually, the security measures in place will need to be reconsidered accordingly.

Pradeo's mobile security solution suite provides tools to:

- Protect data manipulated on collaborator's **managed devices** (COPE, COBO, BYOD...)
- Protect data manipulated on **non-managed devices** (clients, partners, some collaborators...)
- Protect data manipulated in **mobile applications** (banking app, health app...)

CYBERTHREATS TARGETING MOBILE DATA

The following volumes and trends are based on Pradeo's latest mobile security report.

Along the massive growth of enterprise mobility, cybercriminals looking for valuable data naturally shifted their interest toward mobile devices. Indeed, smartphones and tablets have inherent capabilities that, when exploited illegally, can provide a direct access to all the data they manipulate. Mobile threats can operate at three different layers of a device: **application, network and OS.**

Application threats

Mobile applications are cybercriminals favored vector. They can feature a malware, hence being inherently malicious or they can be entirely sane and either leak the data they manipulate or be vulnerable to attacks. In all cases, and whether they are developed internally or externally, mobile applications have the power to strongly hurt data privacy.

Internal threats

Unexpected behaviors

A mobile application can perform unwanted actions because of the external libraries it hosts (Within an Android app, 1 in 8 libraries are vulnerable to attack. On iOS, the ratio is 1 to 5) or as a result of a development negligence between testing and production. Both can lead to silent data leakage and potentially unwanted actions.

Vulnerabilities

A vulnerability comes from either the application's source code or from the libraries it hosts. To help developers, hundreds of code vulnerabilities are referenced. However, 3/4 of mobile applications have a vulnerability identified in the OWASP Top 10 exposing them to data leakage and attacks such as Man-In-The-Middle, Denial of Service, etc.

External threats

Malware

A malware is specifically designed to disrupt, damage, or gain authorized access to a legitimate device or data while the victim often remains unaware of the attack. The number of devices infected by malware, such as keylogger, screenlogger, overlay, etc. continues to grow.

Network threats

Unsecured Wifi, Man-In-The-Middle Attacks

The number of public WiFi hotspots worldwide has increased by 475% since 2016 and is forecast to reach 549 million by the end of 2022 according to a Statista study. More and more employees are getting connected outside company perimeters to unprotected networks, exposing critical data in the process. As such, the acceleration of mobility in the last few years has contributed to an increase of network attacks, such as Man-In-The-Middle, a type of attack that happens when an outside entity intercepts or alters a communication between two parties.

Phishing / Smishing attacks

Although mostly targeting computers until a few years ago, phishing attacks have become the 2nd most detected network threat on mobile devices, and 81% of them are now mostly perpetrated through SMS and apps. The phishing technique traps mobile users into clicking on malicious links, opening infected files or downloading malware from emails (sent from spoofed email addresses) or SMS (smishing) in order to steal the sensitive data they hold.

The rise in phishing can be explained by the fact that it is an inexpensive technique that can simultaneously target a vast amount of people.

Device threats

Outdated / vulnerable OS

On a regular basis, security holes are discovered in the code of operating systems. Once detected, Google and Apple quickly develop patches that they push to users through updates and simultaneously publish documents disclosing the vulnerabilities that existed in the former version. Once made public, cybercriminals can exploit outdated devices' vulnerabilities for their own illicit gain.

When exploited, a vulnerability can provide hackers with extended rights, such as consulting and exfiltrating data or communications. The exploitation of an unpatched vulnerability can lead to system takeover and major data breaches in which confidential details (social security number, credentials, banking details…) are stolen in order to commit identity theft and fraud.

LEGAL FRAMEWORK ENFORCING MOBILE DATA PROTECTION

Personal data

General Data Protection Regulation (GDPR)

The GDPR is a personal data privacy law that applies to any organization that does business in Europe (regardless of its physical location). It sets guidelines for the collection, processing and storage of European residents' personally identifiable information. The GDPR was enforced to protect information belonging to clients, employees, partners and prospects, including the ones that are dealt with on mobile devices and applications.

How does the GDPR apply to mobile data?

Article 5

Personal data shall be processed in a manner that ensures appropriate security, and includes protection against unauthorized processing, accidental loss, destruction or damage.

>> Requires protecting mobile devices and applications on which personal data are handled

Article 25

Organizations shall implement data protection by design, by deploying appropriate solutions which are specifically designed to protect data.

>> Requires implementing security in mobile application development cycles

Article 32

Organizations shall guarantee users' data security commensurately to risk levels by putting in place procedures to regularly test, analyze and evaluate security practices.

>> Requires having visibility on personal data flows and their level of security

Pradeo's mobile security solution suite provides tools to:

- Identify GDPR-sensitive data processing within a mobile fleet
- Reveal mobile applications' actions on GDPR-sensitive data

LEGAL FRAMEWORK ENFORCING MOBILE DATA PROTECTION

Personal data

Country-specific regulations

Personal data privacy regulations such as the GDPR are in effect in various regions of the world, like the **FTC Act (USA), PIPEDA (Canada), DPA (UK), NDB (Australia)** etc. These regulations tend to converge towards the same global guidelines, by asking organizations to:

- Protect personal data manipulated by mobile devices and applications
- Implement risk mitigation practices
- Prevent data loss and breach
- Monitor data processing activities

Some of these laws provide massive fines in case of non-compliance. For example, Instagram was fined €405 million over its 2022 data breach by the Ireland's Data Protection Commission (DPC) and the European Data Protection Board (EDPB).

Pradeo's mobile security solution suite provides tools to:

- Identify sensitive data processing within a mobile fleet
- Reveal mobile applications' actions on sensitive data

LEGAL FRAMEWORK ENFORCING MOBILE DATA PROTECTION

Financial data

Payment Service Directive 2 (PSD2)

The PSD2 applies to banks, payment service providers (PSP) and any other company that handles financial data. It is a European law that enforces the security of mobile banking / payment applications, mobile wallets and all the shopping apps that offer a payment functionality. It aims at harmonizing the protection of electronic payments and consumers' financial data while promoting innovation and offering better experience to users.

How does the PSD2 apply to mobile data

Two complementary mobile security principles appear among the security measures imposed by **Articles 4, 7, 8 and 9 of the RTS**: strong authentication and secure execution environment.

Financial service providers, including banks, must implement authentication based on a minimum of two factors and a one-time password. In order to ensure strong authentication, the confidentiality of the code and the prevention of fraudulent access are required.

The PSD2 highlights the fact that authentication is reliable only when it is ensured that the communication cannot be intercepted and that the data request sender is the user itself, and not a malware. To ensure strong authentication, the PSD2 requires to secure the execution environment by tracking the security of users' mobile endpoints.

Pradeo's mobile security solution suite provides a tool to:

- Secure mobile applications' execution environment

LEGAL FRAMEWORK ENFORCING MOBILE DATA PROTECTION

Financial data

The Payment Card Industry Data Security Standard (PCI DSS)

The PCI Security Standards Council is a global organization that maintains, evolves and promotes an information security standard for organizations that handle credit card data across the globe. It specifically requires all merchants that use mobile payments to protect cardholder data by maintaining a secure environment.

In its requirements for compliance, the standard states that mobile devices are not necessarily designed to be secure.

How does the PCI DSS apply to mobile data

Requirements 5

Protecting all systems against malware and performing regular updates of anti-virus software (malware can enter a network through numerous ways, including Internet use, employee email, mobile devices or storage devices).

>> **Requires the protection of mobile devices against malicious programs**

Requirement 6

Developing and maintaining secure systems and applications. Vulnerabilities in systems and applications allow unscrupulous individuals to gain privileged access. Security patches should be immediately installed to fix vulnerability and prevent exploitation and compromise of cardholder data.

>> **Requires auditing and fixing mobile application vulnerabilities**

Pradeo's mobile security solution suite provides tools to:

- Protect mobile devices from known and zero-day malware attacks
- Audit mobile applications and remediate their vulnerabilities

LEGAL FRAMEWORK ENFORCING MOBILE DATA PROTECTION

Health data

The Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA applies to healthcare organizations operating the United States. It is a set of security rules that aim at safeguarding the privacy of patients and health plan subscribers. The following administrative safeguards of the Act require the protection of the mobile devices and applications used by healthcare organizations.

How does the HIPAA apply to mobile data

(a)(1)(ii)(D) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(a)(5)(ii)(A) Install periodic security updates. **(B)** Procedures for guarding against, detecting, and reporting malicious software. **(C)** Enable logging and log alerting on critical systems.

(a)(6)(ii) Implement policies and procedures to address security incidents. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

>> **Requires to regularly review information system activity, implement solutions to detect and mitigate security incident (including malicious software), alert in case of security incident.**

Pradeo's mobile security solution suite provides a tool to:

- Protect mobile devices from malware and data theft
- Protect mobile applications' sensitive data from malware and exfiltration

As every country has its own mobile data privacy rules, this list is not exhaustive. We advise to get acquainted with any local laws that may apply.

How to get visibility on data processing within a mobile environment?

Most security heads encounter difficulties qualifying and quantifying threats surrounding their mobile environment. Besides, many researches have shown that organizations cannot say with certainty what information their mobile applications manipulate or what data their collaborators have on their mobile device. This lack of visibility can easily lead to the loss or theft of data, endangering compliance to privacy laws and potentially exposing critical data.

Assess the threats targeting mobile devices and applications

Sometimes, organizations are wondering how threatening their mobile environment is and whether they should invest in mobile security solutions. Pradeo Security can be deployed as a **threat intelligence collector** to gather mobile security events and attack logs from managed mobile devices (mobile fleet) or non-managed mobile devices (clients, partners…) and obtain visibility onto an existing threat landscape.

Identify data processing within a mobile fleet

Identifying what data are manipulated on collaborators' mobile devices can be achieved through the deployment of a **Mobile Threat Defense** agent, such as Pradeo Security. Pradeo Security MTD solution relies on a behavioral analysis engine that precisely qualifies all actions performed on data handled on mobile devices, including by mobile applications.

Reveal mobile applications' actions on data

A mobile application can be compared to an iceberg, as most of its behaviors are performed in the background unbeknownst to the users. Those silent behaviors can be uncovered with a **Mobile Application Security Testing** solution such as Pradeo Security, that reveals applications’ behaviors and vulnerabilities.

How to ensure the security of the data accessed by mobile collaborators?

Hospitals, banks, governments and other organizations' members benefit from the great agility brought by mobility, by consulting emails, files, calendars, etc. through tablets, smartphones and applications. But as a consequence, it has become very difficult for IT teams to monitor data privacy.

Mobile device management vendors such as VMware Workspace ONE, IBM MaaS360, Microsoft Intune, BlackBerry UEM, etc. promote **Mobile Threat Defense** integrations within their platforms to fully protect data accessed by mobile devices.

Pradeo Security MTD technology allows identifying and blocking threats in real time on users' devices and to automatically synchronize lists of uncompliant devices and applications on the mobile device management platform. It protects personal and corporate data from malwares and exfiltration.

How to deliver secure mobile services to non-managed devices?

Sometimes, organizations choose not to equip their employees with mobile devices, preferring to adopt a "bring your own device" (BYOD) policy. But collaborators using their personal smartphones for professional purpose may not allow their employer to enroll their device to manage them. Hence, they end up non-managed while accessing corporate data.

To provide mobile services to collaborators using non-managed devices, Pradeo Security is the only mobile security vendor to offer a **secure private application stores**. These stores allow organizations to both distribute business applications and protecting the data they handle, without having to manage a mobile fleet nor engaging internal development processes.

How to ensure the security of the data manipulated by a mobile app?

Once distributed to the public, mobile applications (banking, health, retail…) run on non-managed devices that are potentially compromised or hosting malwares. Mobile applications need to be properly shielded to face threats coming from their execution environment, to keep safe the sensitive data they manipulate.

In-app Threat Defense solutions such as Pradeo Security SDK protect mobile applications from the inside out. Once integrated into an application, the SDK diagnoses its environment and collects security events (connected to SIEMs), allowing companies to get a deeper knowledge of the threats surrounding their app and improve preventive and curative actions. Then, it detects unwanted and malicious behaviors performed on the devices hosting the app and offers an automated and adapted security response.

ABOUT PRADEO MOBILE SECURITY

Pradeo is a global leader of mobile security. It provides mobile threat intelligence services as well as solutions to protect the data handled through smartphones, tablets and mobile applications.

Pradeo developed Pradeo Security, a patented mobile security technology that uses Artificial Intelligence and machine learning to automatically detect and ward off known, unknown and advanced mobile threats including zero-days. Pradeo Security has been recognized as one of the most advanced mobile security technology by Gartner, IDC, Forrester and Frost & Sullivan. It provides a reliable detection of mobile threats to prevent data leakage and reinforce compliance with data privacy regulations.

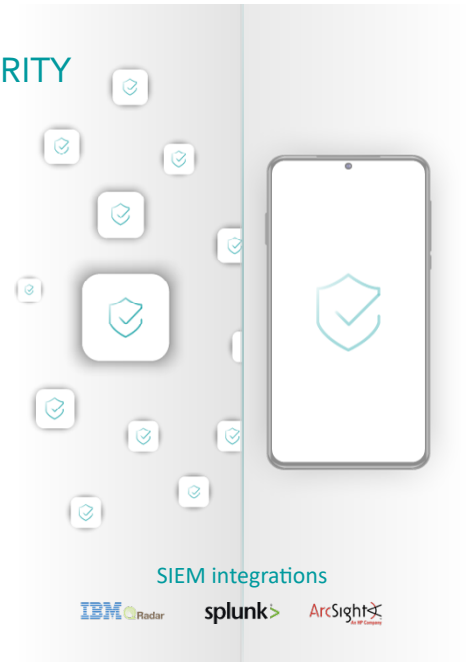
Pradeo Security offers a complete and automatic **protection of the data manipulated by mobile devices and applications**, aligned with organizations' security policy, while preserving business agility.

MOBILE APPLICATION SECURITY

Mobile App Security Testing
Behavior and vulnerability detection, remediation

Shielding
Obfuscation
Encryption
Tamper protection

App Runtime Protection
In-app Threat Defense
App authentication (anti-clone)
Security event collection



MOBILE DEVICE SECURITY

Mobile Threat Defense
Mobile security application
On-device threat detection and response

UEM integrations
Microsoft
Workspace ONE UEM
SAMSUNG Knox Manage
SAMSUNG SDS
BlackBerry
IBM MaaS360
ivanti
SOTI

WORKSPACE SECURITY

Secure Private Store
White-label application store
Security-based conditional access

For more details, visit www.pradeo.com or write to contact@pradeo.com.