



# Corporate Mobile Security Essentials

RISKS, ATTACKS, AND PROTECTION IN BUSINESS CONTEXTS

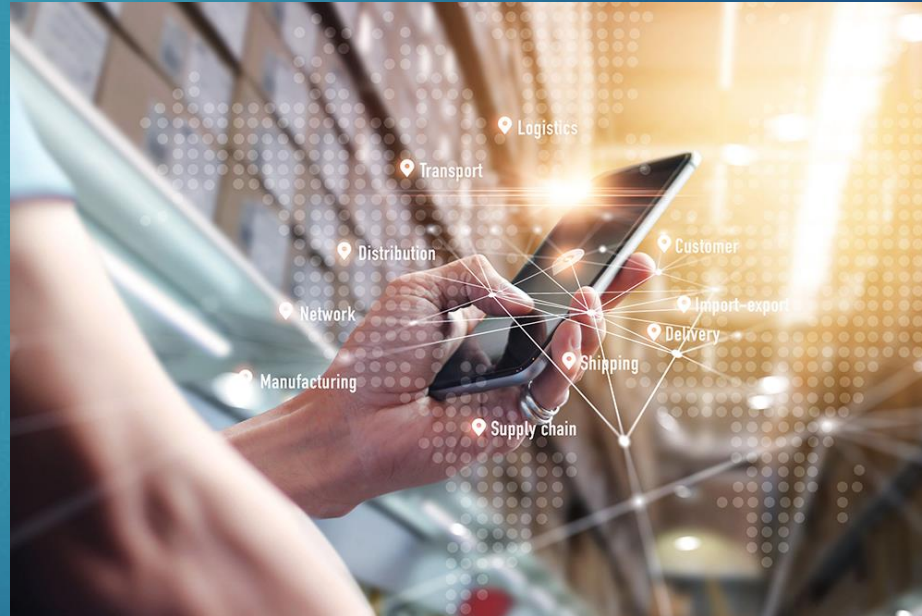
DR. GÖKHAN BAL | GUEST LECTURE | MOBILE BUSINESS 2 | SUMMER 2025

# About Me – Dr. Gökhan Bal

- ▶ **2009:** Degree in Computer Science (Diplom-Informatiker), Goethe University
- ▶ **2015:** Dr. rer. Pol, Goethe University (Chair of Mobile Business & Multilateral Security, Prof. Dr. Kai Rannenbergl)
- ▶ **2015-2024:** Cybersecurity Governance & Consulting @ Deutsche Bahn
- ▶ **Since 10/2024:** Team Lead Cybersecurity Consulting @ AONIC GmbH

# Mobile Devices in the Crosshairs – Why Mobile Security Matters

- ▶ 70% of employees regularly use their smartphone for work-related tasks (IDC, 2024)
- ▶ 60% of successful phishing attacks now occur via mobile devices (Lookout, 2024)
- ▶ 1 in 10 corporate mobile devices is compromised without detection (Verizon DBIR 2024)
- ▶ BYOD + Hybrid Work = new attack surface, often insufficiently secured
- ▶ Mobile devices are often the weakest yet most overlooked point in corporate IT today.



# Mobile Devices – Distinctive Characteristics



- ▶ Always online, constantly carried – increased attack surface
- ▶ Combination of work and personal use (dual use)
- ▶ Access to a wide range of sensitive data: contacts, calendar, emails, location, camera, microphone, authenticator apps
- ▶ Many sensors & interfaces (e.g., NFC, Bluetooth, Wi-Fi, GPS) – new attack vectors
- ▶ Operating systems with distinct architectures (e.g., app sandboxing)

# Threats to Mobile Devices in the Corporate Context

- ▶ Phishing, Smishing, Quishing – specifically tailored to mobile platforms
- ▶ Malware via app stores and APKs (e.g., banking trojans)
- ▶ Data leakage through insecure apps or shadow IT
- ▶ Loss or theft of the device
- ▶ Man-in-the-middle attacks via public networks
- ▶ Zero-day exploits such as Pegasus or Android rootkits



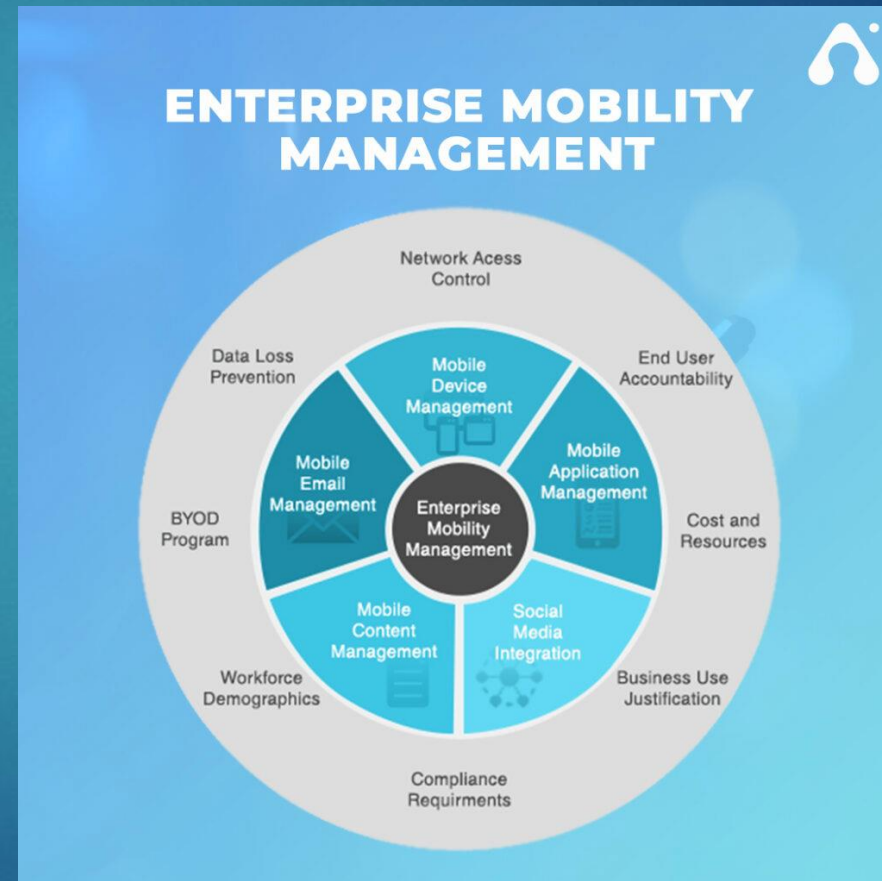
# Usage Models – BYOD, COPE, COBO, CYOD

- ▶ BYOD (Bring Your Own Device): Maximum freedom but high risks
- ▶ COPE (Corporate Owned, Personally Enabled): Good compromise between control and usability
- ▶ COBO (Corporate Owned, Business Only): Maximum security, minimal flexibility
- ▶ CYOD (Choose Your Own Device): Selection from pre-approved devices
- ▶ Decision depends on security requirements, user acceptance, budget, and IT strategy



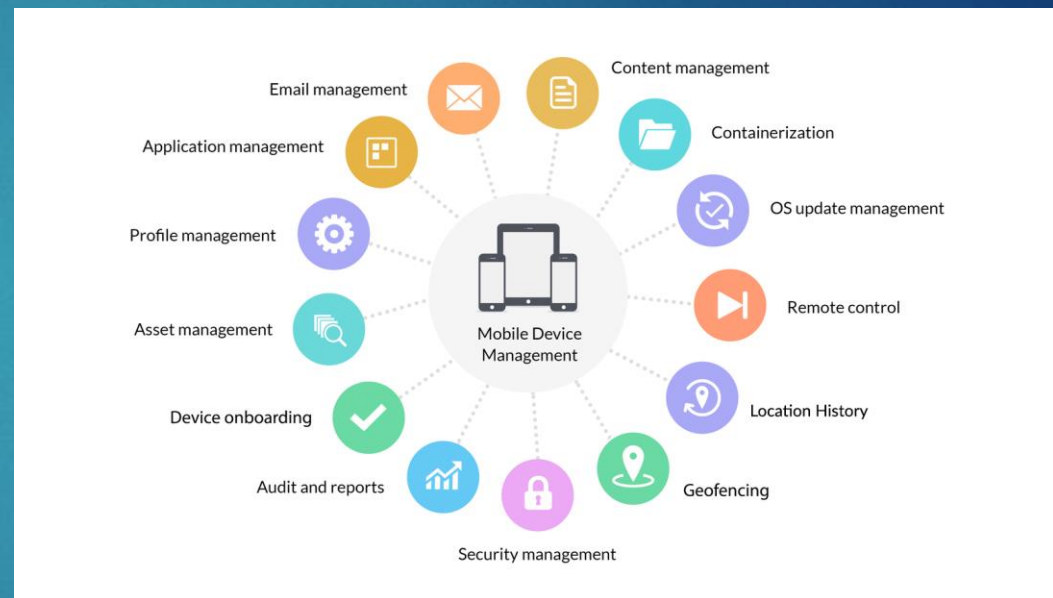
# Enterprise Mobility Management (EMM) – Overview

- ▶ Holistic approach to managing mobile devices within the company
- ▶ Goal: Protect corporate data while supporting mobile productivity
- ▶ Components:
  - ▶ Mobile Device Management (MDM)
  - ▶ Mobile Application Management (MAM)
  - ▶ Mobile Content Management (MCM)
  - ▶ Identity & Access Management (IAM)
- ▶ Integration with existing IT and security infrastructures



# Mobile Device Management – Overview of Functions

- ▶ Device Registration & Inventory
- ▶ Enforcement of Security Policies (e.g., password, encryption)
- ▶ Remote Wipe, Lock, Reset
- ▶ App Distribution and App Blacklist/Whitelist
- ▶ Containerization and Separation of Business/Personal Data
- ▶ Geofencing and Usage Control
- ▶ Compliance Monitoring & Reporting



# Mobile Attack Techniques – Overview & Examples



- ▶ Phishing Variants:
  - ▶ SMishing (via SMS)
  - ▶ Quishing (QR codes)
  - ▶ Vishing (voice calls)
- ▶ Malware via fake apps (e.g., banking trojans like Cerberus)
- ▶ Rogue WiFi Access Points (e.g., Evil Twin)
- ▶ App Permissions Abuse – legitimate apps with hidden spying functions
- ▶ Jailbreaking/Rooting to bypass security

# Pegasus – The Super Spy in the Smartphone

- ▶ State-sponsored spyware by the NSO Group
- ▶ Infection via zero-click exploits (e.g., iMessage, WhatsApp)
- ▶ Access to microphone, camera, chats, location, passwords – completely invisible
- ▶ Proven use against journalists, activists, and politicians worldwide
- ▶ Example of highly sophisticated, state-backed mobile threats



# MITRE ATT&CK Mobile Framework

- ▶ MITRE ATT&CK Mobile is a publicly accessible knowledge base of known attacker techniques targeting mobile platforms (iOS & Android).
- ▶ The framework covers all phases of an attack – from Initial Access through Execution to Exfiltration.
- ▶ Ideal for threat modeling, risk analysis, and security awareness training.
- ▶ Supports mapping real-world attacks to known techniques
- ▶ (e.g., Pegasus uses zero-click exploits and privilege escalation among others).



# MITRE ATT&CK Mobile Framework

Home > Matrices > Mobile > Mobile

## Mobile Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Mobile. The Matrix covers techniques involving device access and network-based effects that can be used by adversaries without device access. The Matrix contains information for the following platforms: Android, iOS.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side ▾ show sub-techniques hide sub-techniques help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
8 techniques	4 techniques	7 techniques	3 techniques	17 techniques	5 techniques	8 techniques	2 techniques	13 techniques	9 techniques	2 techniques	10 techniques
Application Versioning	Command and Scripting Interpreter (1)	Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism (1)	Application Versioning	Access Notifications	File and Directory Discovery	Exploitation of Remote Services	Access Notifications	Application Layer Protocol (1)	Exfiltration Over Alternative Protocol (1)	Account Access Removal
Drive-By Compromise	Exploitation for Client Execution	Compromise Application Executable	Exploitation for Privilege Escalation	Download New Code at Runtime	Clipboard Data	Location Tracking (2)	Replication Through Removable Media	Adversary-in-the-Middle	Call Control	Exfiltration Over C2 Channel	Call Control
Exploitation for Initial Access	Native API	Compromise Client Software Binary	Process Injection (1)	Execution Guardrails (1)	Credentials from Password Store (1)	Network Service Scanning		Archive Collected Data	Dynamic Resolution (1)		Data Destruction
Lockscreen Bypass	Scheduled Task/Job	Event Triggered Execution (1)		Foreground Persistence	Input Capture (2)	Process Discovery		Audio Capture	Encrypted Channel (3)		Data Encrypted for Impact
Phishing		Foreground Persistence		Hide Artifacts (3)	Steal Application Access Token (1)	Software Discovery (1)		Call Control	Ingress Tool Transfer		Data Manipulation (1)
Replication Through Removable Media		Hijack Execution Flow (1)		Hooking		System Information Discovery		Clipboard Data	Non-Standard Port		Endpoint Denial of Service
SIM Card Swap		Scheduled Task/Job		Impair Defenses (3)		System Network Configuration Discovery (2)		Data from Local System	Out of Band Data		Generate Traffic from Victim
Supply Chain Compromise (3)				Indicator Removal on Host (3)		System Network Connections Discovery		Input Capture (2)	Remote Access Software		Input Injection
				Input Injection				Location Tracking (2)	Web Service (3)		Network Denial of Service
				Masquerading (1)				Protected User Data (4)			SMS Control
				Native API				Screen Capture			
				Obfuscated Files or Information (2)				Stored Application Data			
				Process Injection (1)				Video Capture			
				Proxy Through Victim							
				Subvert Trust Controls (1)							
				Virtualization Solution							
				Virtualization/Sandbox Evasion (1)							

# MITRE ATT&CK Mobile Framework

MITRE | ATT&CK

Matrices - Tactics - Techniques - Defenses - CTI - Resources - Benefactors

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. To potentially join us on stage, submit to our CFP by July 9th

Home > Techniques > Mobile > Phishing

## Phishing

Adversaries may send malicious content to users in order to gain access to their mobile devices. All forms of phishing are electronically delivered social engineering. Adversaries can conduct both non-targeted phishing, such as in mass malware spam campaigns, as well as more targeted phishing tailored for a specific individual, company, or industry, known as "spearphishing". Phishing often involves social engineering techniques, such as posing as a trusted source, as well as evasion techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages.

Mobile phishing may take various forms. For example, adversaries may send emails containing malicious attachments or links, typically to deliver and then execute malicious code on victim devices. Phishing may also be conducted via third-party services, like social media platforms.

Mobile devices are a particularly attractive target for adversaries executing phishing campaigns. Due to their smaller form factor than traditional desktop endpoints, users may not be able to notice minor differences between genuine and phishing websites. Further, mobile devices have additional sensors and radios that allow adversaries to execute phishing attempts over several different vectors, such as:

- SMS messages: Adversaries may send SMS messages (known as "smishing") from compromised devices to potential targets to convince the target to, for example, install malware, navigate to a specific website, or enable certain insecure configurations on their device.
- Quick Response (QR) Codes: Adversaries may use QR codes (known as "quishing") to redirect users to a phishing website. For example, an adversary could replace a legitimate public QR Code with one that leads to a different destination, such as a phishing website. A malicious QR code could also be delivered via other means, such as SMS or email. In the latter case, an adversary could utilize a malicious QR code in an email to pivot from the user's desktop computer to their mobile device.
- Phone Calls: Adversaries may call victims (known as "vishing") to persuade them to perform an action, such as providing login credentials or navigating to a malicious website. This could also be used as a technique to perform the initial access on a mobile device, but then pivot to a computer/other network by having the victim perform an action on a desktop computer.

### Procedure Examples

ID	Name	Description
G1028	APT-C-23	APT-C-23 sends malicious links to victims to download the masqueraded application. <sup>[1][2]</sup>
G1002	BITTER	BITTER has delivered malicious applications to victims via shortened URLs distributed through SMS, WhatsApp, and various social media platforms. <sup>[3]</sup>
S1094	BRATA	BRATA has been distributed using phishing techniques, such as push notifications from compromised websites. <sup>[4]</sup>
S1208	FjordPhantom	FjordPhantom has been distributed via email, SMS and other messaging applications. <sup>[5]</sup>
S1067	FluBot	FluBot has been distributed via malicious links in SMS messages. <sup>[6]</sup>
S1185	LightSpy	LightSpy has delivered malicious links through Telegram channels and Instagram posts. <sup>[7][8]</sup>
S0289	Pegasus for iOS	Pegasus for iOS has been distributed via malicious links in SMS messages. <sup>[9]</sup>
G0034	Sandworm Team	Sandworm Team used SMS-based phishing to target victims with malicious links. <sup>[10]</sup>

ID: T1660  
Sub-techniques: No sub-techniques  
Tactic Type: Post-Adversary Device Access  
Tactic: Initial Access  
Platforms: Android, iOS  
MTC ID: AUT-9  
Contributors: Adam Mashinchi; Brian Donohue; Naveen Devaraja, boltech; Sam Seabrook, Duke Energy; Vijay Lalwani; Will Thomas, Equinix  
Version: 1.0  
Created: 21 September 2023  
Last Modified: 29 September 2023  
[Version Permalink](#)

# MITRE ATT&CK Mobile Framework

## Mitigations

ID	Mitigation	Description
M1058	Antivirus/ Antimalware	Some mobile security products offer a loopback VPN used for inspecting traffic. This could proactively block traffic to websites that are known for phishing or appear to be conducting a phishing attack.
M1011	User Guidance	Users can be trained to identify social engineering techniques and phishing emails.

## Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Mobile security products may provide URL inspection services that could determine if a domain being visited is malicious.
		Network Traffic Flow	Enterprises may be able to detect anomalous traffic originating from mobile devices, which could indicate compromise.

## References

1. Kohli, P. (2021, November 23). Android APT spyware, targeting Middle East victims, enhances evasiveness. Retrieved November 17, 2024.
2. CheckPoint Research. (2020, February 16). Hamas Android Malware On IDF Soldiers-This is How it Happened. Retrieved November 17, 2024.
3. BlackBerry Research and Insights Team. (n.d.). Mobile Malware and APT Espionage. Retrieved March 1, 2024.
4. Securelist. (2019, August 29). Fully equipped Spying Android RAT from Brazil: BRATA. Retrieved December 18, 2023.
5. Promon Security Research Team. (2024, October 1). Retrieved February 19, 2025.
6. Europol. (2022, June 1). Takedown of SMS-based FluBot spyware infecting Android phones. Retrieved April 18, 2024.
7. Firsh, A., et al. (2020, March 26). iOS exploit chain deploys LightSpy feature-rich malware. Retrieved January 13, 2025.
8. Shoshin, P. (2020, March 27). LightSpy spyware targets iPhone users in Hong Kong. Retrieved February 12, 2025.
9. Marczak, B., et al. (2020, December 20). The Great iPwn. Retrieved April 3, 2024.
10. Billy Leonard. (2023, April 19). Ukraine remains Russia's biggest cyber focus in 2023. Retrieved March 1, 2024.
11. Microsoft. (2023, October 25). Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction. Retrieved March 18, 2024.
12. Agranovich, D., et al. (2022, April). Adversarial Threat Report. Retrieved April 2, 2024.



# Throwback: Privacy in Smartphone App Ecosystems

FROM OWN PHD RESEARCH (2010-2015)

























# Motivation

## Real-World Case: Brightest Flashlight

250 flashlight apps in



Apps

 <p>Taschenlampe Tiny Nikolay Ananiev</p> <p>★★★★★</p>	 <p>Superhelle LED Taschenlampe Surpax Technology Inc.</p> <p>★★★★★</p>	 <p>TaschenLampe LED smallte.ch</p> <p>★★★★★</p>	 <p>Taschenlampe Zerone Mobile Inc.</p> <p>★★★★★</p>	 <p>Taschenlampe- Flashlight Mobile Apps Inc.</p> <p>★★★★★</p>	 <p>Hellste LED Taschenlampe Intellectual Flame Co., Ltd.</p> <p>★★★★★</p>	 <p>Taschenlampe LED Notes</p> <p>★★★★★</p>	 <p>Taschenlampe SlimGears</p> <p>★★★★★</p>
 <p>Galaxy S5 Taschenlampe Flashlight Team</p> <p>★★★★★</p>	 <p>Taschenlampe + Uhr Flashlight + Clock</p> <p>★★★★★</p>	 <p>Taschenlampe Zentertain</p> <p>★★★★★</p>	 <p>Tolle Helle Taschenlampe iHandy Inc.</p> <p>★★★★★</p>	 <p>Taschenlampe Stefan Fabian</p> <p>★★★★★</p>	 <p>Brightest Taschenlampe GoldenShores Technol</p> <p>★★★★★</p>	 <p>Spicy Taschenlampe SPICY SOFTWARE</p> <p>★★★★★</p>	 <p>Taschenlampe: LED Mobile Apps Inc.</p> <p>★★★★★</p>
							

# Motivation

## Real-World Case: Brightest Flashlight



**Brightest Taschenlampe**  
GoldenShores Technologies, LLC - 19. Dezember 2013  
Tools

Installiert

*i* Diese App ist mit allen Ihren Geräten kompatibel.

★★★★★ (1.166.094) g+1 +186961 Auf Google empfehlen

Beschreibung	Weitere Informationen		
Brightest Taschenlampe - kostenlos	<b>Aktualisiert</b>	<b>Größe</b>	<b>Installationen</b>
* Schaltet alle verfügbaren Lichter auf dem Gerät	19. Dezember 2013	1,2M	50.000.000–100.000.000
* Kamerablitz auf Maximum * Screen LED am Max			
* Tastaturbeleuchtung auf Maximum			
* Soft-Tasten-Hintergrundbeleuchtung auf LED-Anzeige			
* Maximale bei Maximum			
* Automatische Timer Exits Anwendung nach 120 Sekunden			
* Audio-Effekte auf Start und Stop			
* unaufdringliche Anzeigen			



# Motivation

## Real-World Case: Brightest Flashlight

18

06.12.2013 15:53  « Vorige | Nächste »

vorlesen / MP3-Download

Eine Taschenlampen-App für Android-Handys hat unerlaubt Daten über Aufenthaltsort und Gerät der Nutzer gespeichert und an Werbenetzwerke weitergegeben. Die App wurde mindestens 50 Millionen Mal aus Googles Play-Store heruntergeladen. Die App habe Nutzer nicht darüber informiert, dass deren Aufenthaltsort und die Identifikationsnummer der Geräte an Dritte weitergegeben wurden, erklärte die US-Handelsbehörde FTC, die sich mit der Betreiberfirma außergerichtlich einigte.

Nach dem Herunterladen der Anwendung hätten Handynutzer die Möglichkeit gehabt, einer Datenübertragung zuzustimmen oder sie abzulehnen. Allerdings wurden bereits Daten übertragen, bevor die Nutzer eingewilligt hatten. Außerdem hätten die Hersteller nicht erwähnt, dass gesammelte Daten nicht nur von ihnen selbst verarbeitet, sondern auch an Dritte weitergereicht wurden.

Der App-Entwickler **Goldenshores Technologies** muss nun alle persönlichen Daten, die über die Taschenlampen-App gesammelt wurden, löschen. Außerdem muss er die Datensammlung transparent machen und eine explizite Einwilligung der Nutzer einholen.



# Motivation

## Real-World Case: Brightest Flashlight

### Avoidable? Risk of Infringement?



Brightest Taschenlampe  
requires access to:

- Location**
- Pictures/Media/Files
- Camera/Microphone
- Network Connection Information
- Device ID / Call Information
- Bluetooth Information

Google play ACCEPT

Bewertung schreiben

Premankur Sukul ★★★★★  
Spy. It transmits user's real time location to ad networks and other third parties.. Basically its a stalking device

Pascal L. ★★★★★  
-.- Eine Taschenlampe mit derartigen Rechtforderungen?? Hallo?? Wozu will eine TASCHENLAMPE!!! meinen

Angeboten von GoldenShores Technologies, LLC

**"Uninstall immediately!!!!!!!"**  
According to "Süddeutsche Zeitung" from 6.12.2013, this app reads data and shares...

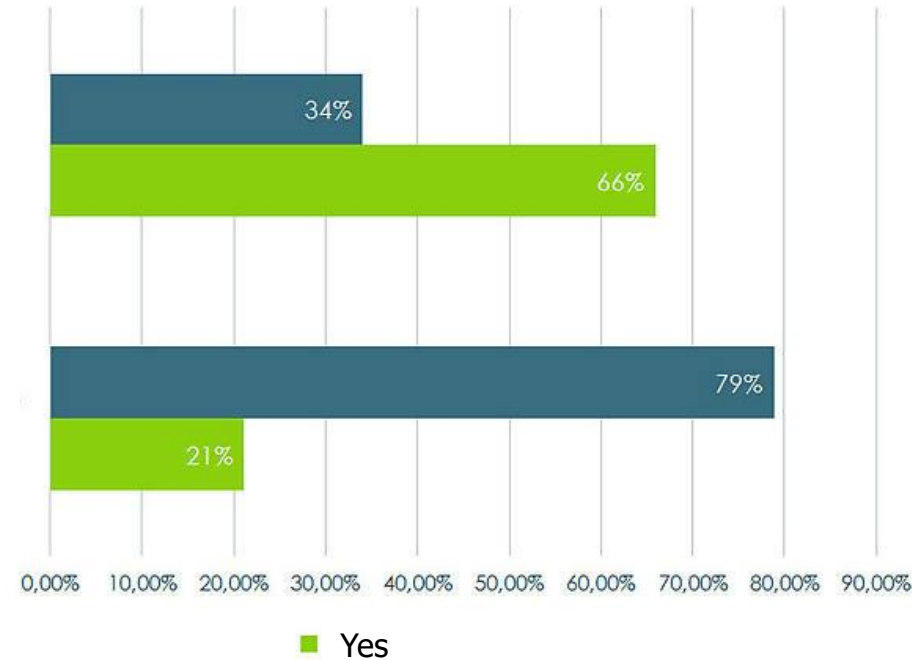
[Privacy Policy](#)

of the Brightest Flashlight® privacy policy is contained within the...  
A flashlight app with such permission requests?? Hello?? Why would a FLASHLIGHT want my...

TRANSMISSION OF GEOLOCATION INFORMATION  
GoldenShores Technologies and its subsidiaries and agents may collect your geolocation based information and transmit that information to third-party service providers. Geolocation includes data regarding your device's location, including but not limited to...

**Do you inform yourself about the requested permissions before installation?**

**Do you feel well-informed about why an app requests certain permissions?**



**media Test digital**

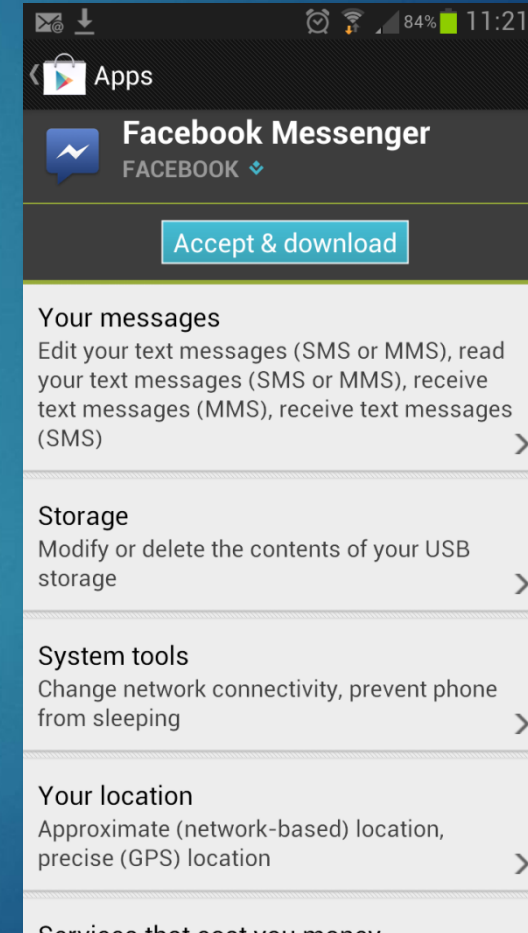
[http://www.focus.de/digital/gastkolumnen/haller/umfrage-zu-datenschutz-user-nutzen-smartphone-apps-zu-leichtsinnig-\\_aid\\_1062985.html](http://www.focus.de/digital/gastkolumnen/haller/umfrage-zu-datenschutz-user-nutzen-smartphone-apps-zu-leichtsinnig-_aid_1062985.html)

# Motivation

21

## Current privacy risk information is...

- ▶ ... static,
- ▶ ... coarse-grained & technical,
- ▶ ... timed inappropriately,
- ▶ ... ignored largely,
- ▶ ... **not an effective measure to inform users about individual privacy risks of apps.**





Vielen Dank!

[MAIL@GOEKHANBAL.DE](mailto:MAIL@GOEKHANBAL.DE)