International Journal of Scientific Research in Computer Science and Engineering
Vol.**12**, Issue.**1**, pp.**42-52**, February **2024**
E-ISSN: 2320-7639
Available online at: www.isroset.org

Research Article

Evaluating the Permissions of Monitoring Mobile Applications for Remote Employees: Analysing the Impact on Employer Trust and Employee Privacy Concerns

Polra Victor Falade[1*], Patience Ocheche Momoh[2]

[1]Dept. of Cyber Security, Nigerian Defence Academy, Kaduna, Nigeria
[2]Postgraduate Diploma Student, Nigerian Defence Academy, Kaduna, Nigeria

**Corresponding Author: pvfalade@nda.edu.ng*

Received: 27/Dec/2023; **Accepted**: 25/Jan/2024; **Published**: 29/Feb/2024

Abstract— Amid the worldwide COVID-19 pandemic, there has been an extraordinary surge in remote work, bringing attention to its lasting effects on the modern workforce. This significant change has led organizations to adopt remote work as a permanent element, requiring them to develop flexible and robust work approaches. Amidst the exponential growth of remote work, the use of monitoring apps to oversee employee tasks has become more common. However, the widespread adoption of these apps has raised significant concerns about the privacy of data and the rights of employees. This study focuses on examining the privacy problems associated with monitoring mobile apps designed for remote workers. We looked at 12 such apps. To evaluate the privacy concerns associated with mobile applications used for monitoring remote employees, we employed a vulnerability assessment tool. Surprisingly, all 12 apps lacked privacy policies, and also all had permissions that could potentially violate employees' privacy by revealing sensitive information about them. This research provides important insights into the areas of data privacy, employee monitoring, and remote work practices. It offers guidance to app developers and organizations on how to strike a balance between monitoring productivity and protecting employee privacy rights. By addressing the issues raised in this study, stakeholders can create a safe and supportive environment for remote workers while still respecting their privacy and building trust.

Keywords— Employee monitoring, mobile applications, remote work, privacy issues, trust

1. Introduction

In the contemporary swiftly changing digital terrain [1], [2], the convergence of mobile technology and remote work has reshaped the way organizations operate [3]. As businesses strive to maintain productivity and connectivity in an increasingly decentralized workforce, the utilization of mobile applications to monitor remote employees has gained prominence [4]. These applications offer the potential to track work-related activities, enhance communication, and ensure task completion, thereby fostering efficiency and accountability. However, this technological advancement raises critical concerns about individual privacy [5].

This research assesses employee monitoring mobile applications for privacy issues and delves into the intricate interplay between the imperative for efficient remote workforce management and the fundamental right to privacy. As organizations implement monitoring mechanisms through mobile applications, a range of privacy considerations emerges [5]. This study undertakes a comprehensive examination of the multifaceted dimensions of this issue, aiming to shed light on the ethical, legal, and socio-economic implications of monitoring practices.

This research sets the stage for a rigorous exploration of the topic, highlighting the tension between organizational goals and individual privacy rights. By critically evaluating the potential benefits and risks associated with monitoring mobile applications for remote employees, this research aims to provide valuable insights for businesses, policymakers, and individuals alike. Through a balanced analysis of perspectives, this study contributes to the ongoing dialogue surrounding the responsible and respectful implementation of monitoring technologies in the modern era of remote work.

2. Remote Work

Amid the global COVID-19 pandemic, remote work has undergone an unprecedented surge, casting a spotlight on its enduring implications for the contemporary workforce [6]. This transformative shift has prompted organizations to

embrace remote work as a permanent fixture, demanding adaptable and resilient work strategies [6]. Notably, the pandemic has illuminated remote work's potential to reshape fundamental paradigms of work [7]. Moreover, the escalating demand for specialized skills, particularly within the tech sector, underscores the allure of remote work. In regions such as Brazil, the United States, China, Japan, and Southeast Asia, talent scarcity has become a palpable challenge, while India presents a promising remote workforce reservoir [8]. Remote work's unique offering of flexibility and autonomy addresses skill shortages and concurrently fosters enhanced employee well-being and productivity [8]. Furthermore, the notion of remote work has transcended the bounds of the traditional office, encompassing versatile settings like shared workspaces and personalized offices [9]. As eloquently put by Jalagat [10], remote work has evolved to encompass telecommuting and virtual work, effectively surpassing conventional office-based norms [10].

Importantly, the appeal of remote work extends beyond immediate exigencies, offering benefits to both employers and employees [11]. The rapid pivot to remote work during the pandemic has underscored its adaptability and driven organizations to reassess their work models [12]. Remote work acceleration was catalyzed by businesses aiming to maintain operations while ensuring the well-being of employees [6]. While initially limited in scope, remote work's broader relevance has solidified, showcasing its potential as a transformative work mode [13]. Nonetheless, optimizing remote work arrangements remains a challenge that organizations must navigate to unlock its full potential [13].

Interestingly, industries have embraced remote work at varying speeds, revealing their adaptability and unique challenges [14]. The technology and telecommunications sector, which is well-acquainted with remote-friendly cultures, has emerged as a vanguard in remote work adoption [14]. In contrast, sectors such as food, drink, retail, and consumer services are undergoing a paradigm shift by integrating remote work policies [14]. Even within the manufacturing sector, traditionally reliant on on-site presence, the exploration of remote work for specific roles underscores the sector's technological adaptability [14]. This transition's pace and character are inevitably influenced by the distinct characteristics of each industry [15].

However, the widespread adoption of remote work has unveiled a new frontier of cybersecurity concerns [13]. The surge in remote work during the pandemic coincided with a substantial uptick in cyberattacks [9]. The expansion of the attack surface due to remote work and public cloud utilization has exacerbated concerns surrounding cybersecurity vulnerabilities [13]. Addressing the security of remote employees and managing these vulnerabilities have emerged as paramount priorities for organizations [16]. The dissolution of conventional office boundaries has exposed businesses to heightened risks of data breaches and cyberattacks [16]. Conventional security measures prove inadequate in safeguarding remote workers, compelling cybercriminals to exploit vulnerabilities inherent to remote work setups [17]. In response, formulating a robust cybersecurity strategy becomes imperative to counter these evolving threats [17], [18].

3. Employer’s Trust Versus Employee’s Privacy Monitoring

In the realm of both business and government, a significant challenge has arisen as they navigate the shift towards a substantial portion of their workforce functioning remotely from home [19]. Recent data released by the United Kingdom (UK) Government underscores the extent of this shift, revealing a 28% to 36% increase in remote online work compared to pre-2020 periods [19]. While grappling with technical intricacies, a crucial managerial challenge emerges - effectively overseeing a workforce seldom seen in person [19]. This situation underscores the vital role of trust within the workplace. The limited face-to-face interactions between supervisors and employees necessitate a thoughtful approach to remote work relationships, crucial for sustaining trust, productivity, and employee well-being [19]. The UK Government agency, the Advisory, Conciliation and Arbitration Service (ACAS) underscores the centrality of trust in fostering positive and productive work relationships, emphasizing its role as a cohesive force [19]. Conversely, the absence of trust can breed feelings of being uninformed, anxious, or uncertain about intentions and motivations [19].

Notably, the COVID-19 pandemic has compelled leaders to pivot into remote management, requiring distinct skills compared to in-person supervision [4]. Often, this transition transpired without adequate training, leaving managers to navigate this new terrain unguided [12]. While certain roles have seamlessly adapted to remote work, various industries are ill-suited for this paradigm, with employees struggling to strike a balance between work and home responsibilities [12]. Consequently, managers may find their responsibilities amplified, further exacerbating the challenges for their subordinates in adapting [19]. Even before the pandemic, managing remote employees posed unique challenges. Studies indicate that managers who cannot physically observe their team may grapple with trusting their engagement levels [4]. Such trust gaps can give rise to unreasonable expectations, potentially leading to employees feeling obligated to be constantly available [4], [19]. The confluence of professional and personal boundaries blurs, triggering disruptions to personal lives and heightened job-related stress [20]. Trust issues in remote management may stem from prior experiences, communication gaps, or perceived lack of transparency [20].

In the pursuit of effective remote management, employers are increasingly embracing monitoring applications to oversee remote employees [21]. These tools, tailored for remote monitoring, provide insights into employee activities, productivity, and progress [21]. With a growing remote workforce, organizations are progressively adopting remote monitoring technologies, each serving specific purposes [21]. These apps encompass functions such as keystroke tracking, measurement of active and idle duration on pivotal

applications and websites, and even the capture of photos to validate employees' presence while working from home [21]. The benefits of these monitoring applications for organizations employing remote staff are multi-faceted. Firstly, they ensure accurate tracking of employee work hours, facilitating equitable compensation and compliance with labour laws [4]. Secondly, such apps facilitate visibility into tasks, enabling supervisors to gauge productivity levels and identify avenues for improvement [4]. Thirdly, they streamline project management by promoting efficient collaboration and task allocation within remote teams. Lastly, these tools bolster cybersecurity efforts, mitigating unauthorized access to sensitive company information [4]. Despite these merits, the proliferation of monitoring apps has ignited concerns surrounding employee privacy [5]. The constant scrutiny of remote employees' activities raises questions regarding the delineation between professional responsibilities and personal life [5]. The invasive nature of these apps, including screenshot capture and website tracking, can foster discomfort and distrust among employees. Remote workers may feel as though their every move is under scrutiny, potentially increasing stress and negatively impacting mental well-being [5].

Nonetheless, the utilization of tracking tools carries inherent risks. Workplace surveillance is subject to regulations outlined by federal and state statutes, which delineate instances where employees retain a reasonable expectation of privacy and stipulate requirements for informing employees about monitoring practices [21]. Disclosing surveillance to employees removes their reasonable expectation of privacy, an important legal safeguard. Beyond legal considerations, transparency about monitoring is pivotal for establishing trust within the workforce, addressing privacy concerns, and striking a balance between productivity and privacy [5].

The adoption of monitoring applications can pose challenges to achieving work-life balance. The fusion of work and personal life can strain employees' ability to disconnect and engage fully in personal pursuits [22]. Moreover, the reduced social interaction characteristic of remote work can lead to feelings of isolation and loneliness, further undermining work-life balance. Additionally, the extensive collection and storage of sensitive employee data by monitoring apps raise issues regarding unauthorised access and data breaches. Robust data security measures are essential to safeguard this information from cyber threats [12].

Mobile applications, software programs designed to operate on mobile devices, have gained traction across industries, revolutionizing the global Information and Communication Technology landscape [23]. Offering ease of use, affordability, and compatibility across diverse mobile phones, mobile apps boast a wide range of functionalities, from communication to entertainment [23].

Monitoring mobile apps encompasses the practice of using software to track and observe the activities and usage of mobile applications on devices such as smartphones and tablets [24]. This monitoring yields valuable insights into how individuals engage with their mobile devices and serves various objectives, from employee oversight to parental control and security enhancement [25].

Despite the growing attention to employee monitoring and privacy, gaps remain in comprehending the comprehensive privacy implications of monitoring apps for remote workers. Existing research predominantly focuses on specific aspects, such as productivity or legal compliance, underscoring the need for an all-encompassing and in-depth examination. As remote work continues shaping modern work dynamics, the utilization of monitoring apps for employee surveillance is poised to persist. To ensure their ethical and sustainable deployment, a thorough evaluation of their privacy implications is indispensable. This research aims to contribute to the existing corpus of knowledge by offering a comprehensive analysis of the privacy concerns stemming from monitoring apps for remote workers. In doing so, organizations can make informed decisions that prioritize both privacy and productivity.

4. Research Methodology

To evaluate the privacy concerns associated with mobile applications used for monitoring remote employees, we employed a vulnerability assessment tool, Immuniweb. This tool was selected due to its capacity to uncover privacy-related issues within mobile applications, encompassing aspects such as privacy policies and application permissions [26]. Furthermore, its accessibility, no-cost availability, and user-friendliness made it an appropriate choice for our study.

ImmuniWeb boasts a comprehensive array of features aimed at fortifying the security posture of web and mobile applications. Firstly, its automated Vulnerability Scanning functionality meticulously scrutinizes applications and APIs for prevalent security vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) [27]. Supplementing this automated approach, ImmuniWeb offers Manual Penetration Testing conducted by its security experts to unearth nuanced security flaws that automated tools might overlook [27].

Moreover, the platform evaluates applications against the Open Web Application Security Project (OWASP) Top 10, a benchmark representing the most pressing security risks in web applications. Beyond mere vulnerability assessment, ImmuniWeb extends its purview to Compliance Testing, ensuring adherence to regulatory standards such as the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). For mobile applications, both Android and iOS, ImmuniWeb provides dedicated Mobile Application Security Testing to uncover potential code vulnerabilities [27].

Continuous Monitoring as one of the key features facilitates ongoing scrutiny, enabling organizations to promptly identify and rectify newly emerging vulnerabilities. Detailed Security Reports generated by ImmuniWeb furnish comprehensive insights into identified vulnerabilities, their severity levels,

and recommended remediation measures [27]. Additionally, the platform offers Secure Development Training, empowering developers with the knowledge and resources to construct more resilient applications while averting common security pitfalls. Through its multifaceted features, ImmuniWeb endeavours to bolster the security fabric of digital assets and fortify organizational defences against evolving cyber threats [27].

Our assessment focused solely on the Android versions of employee monitoring mobile applications. This choice was motivated by the widespread use of devices operating on the Android Operating System, which is known to have a higher susceptibility to vulnerabilities and cyber-attacks [6]. We opted to evaluate applications in a randomized manner, considering the considerable variety of employee monitoring apps available, each with distinct functionalities. Notably, numerous monitoring apps serve purposes other than employee monitoring, such as parental control or partner surveillance. It's essential to clarify that our study's scope is restricted to employee monitoring apps. An overview of the 12 monitoring mobile applications scrutinized during this research is presented in Table 1. These applications encompass a range of monitoring functions, including time tracking, location tracking, social media tracking, call and message monitoring, screen recording, screen captures, and file access. The chosen applications collectively cover the major functionalities commonly found in employee monitoring applications.

To proceed, we obtained the Android Package Kit (APK) file for each monitoring mobile application, which we downloaded from https://en.uptodown.com/android/security-performance. Subsequently, we uploaded these APK files onto the ImmuniWeb Mobile platform (https://www.immuniweb.com/mobile/) for comprehensive scanning [28], [29]. The scanning process on ImmuniWeb Mobile involved the following steps [26]:

a. Registering an account using a company email address.
b. Logging into the created Immuniweb account.
c. Uploading the APK file of the respective application.
d. Automatic initiation of the scanning process upon upload.
e. Downloading the generated report upon the scan's completion.

The obtained scan report contained a range of insights, including details about privacy and permissions, external communication, component analysis, and the identification of OWASP's top ten vulnerabilities. For this paper, we focused on the privacy and permissions section of the report, which aligned with the objectives of our study. This approach enabled us to extract pertinent information that sheds light on the privacy implications associated with the assessed monitoring of mobile applications.

Table 1: Monitoring mobile applications

Name of APP	Functionalities	App ID/Version	Test Runtime	No of Downloads
Chat Tracker	Track WhatsApp usage, and monitor online behaviour	online.chat.tracker/1.0.10	13 mins	500k
Eyezy	Secretly monitors mobile phone activities; tracks call logs & text messaging, location, and private search history and finds files	com.eyezy.android/1.1.6	8 mins	500k
Message and Call Tracker	Monitors both outgoing and incoming messages and calls	com.gcm_call_sms_tracker.updat/1.20	11 mins	1M
Mobile Tracker	Tracks users' activities over communication platforms such as text messages, Facebook, and WhatsApp, captures photos, and retrieves deleted images.	com.mobiletracker.mobileapp/ 8.0	4 mins	1M
Desktime mobile time tracker	Automatic monitoring of freelancers and team productivity, real-time tracking of website and app usage	desktime.main/ 3.3.1	5 mins	10k
Employee time tracker (Apploye)	Tracking locations, work time recording and monitoring screen activities	com.apploye.employeetimetrac/ 1.0.3	6 mins	100k
Track team manager	Real-time tracking of team members' locations, push notifications, attendance and live chat	com.trackteam.office.Manager/ 2.7	5 mins	500k
Quick books time tracking	Time tracking, overtime alerts and generating a report on labour expenses.	Com.tsheets.android.hammerhe/ 3.98.2.20230424.1.RELEASE	18 mins	1M
Hubstaff time and hours tracker	Track employees' working hours, logged-in time, total time to complete a project, duration spent on the computer and capture screen activity	Com.netsoft.Hubstaff/ 2.1.12	8 mins	100k
Workganizer time tracking	Time tracking, capturing screenshots of work progress, detailed reports, record keeping and seamless tracking in offline or idle mood.	com.webbiner.workganizer/ 2.0.0	14 mins	10k
Net monitor for employees	Remote monitoring and control of computer systems	com.networklookout/ 5.8.21	3 mins	10k
Chat message tracker remotely	Monitors real-time location, social media tracking and cell phone activities remotely	Com.trackerapps.whatsapptracker/ 1.34	12 mins	1M

5. Results

In this section, we delve into the outcomes of our assessment concerning the mobile applications designed for monitoring remote employees. Our evaluation concentrated on critical facets, specifically the privacy policy and the application permissions associated with these applications. Through examination of these key elements, we aimed to gain a

holistic comprehension of the privacy implications these applications might pose.

5.1 Privacy Policy

A privacy policy functions as a formal declaration or written document outlining the procedures employed by an organization or website to collect, employ, store, and ensure the security of personal data belonging to individuals who interact with their services [30]. However, it is worth noting that within the context of our evaluation of the 12 monitoring mobile applications, a notable observation emerged. Namely, none of the assessed applications possessed a privacy policy in place, highlighting a significant weakness or misconfiguration in terms of privacy practices.

5.2 Monitoring Mobile Application Permissions

Monitoring mobile applications often requires specific permissions to access and monitor various aspects of a user's device and activities. These permissions can vary depending on the app's intended functionality and purpose. In the context of mobile apps, permissions refer to the access and privileges that an app requests from users to perform certain actions or access specific data on their devices. When users install an app, they are usually presented with a list of permissions that the app needs. These permissions outline the resources or information required by the app to function properly or provide specific features. Permissions serve as a mechanism for users to manage and control the level of access granted to the app. By reviewing and granting permissions, users are empowered to make informed decisions regarding the data and functionalities they are comfortable sharing with the app [31].

The classification of permissions into "normal" and "dangerous" is an important distinction. Table 2 gives the normal permissions found across all the assessed applications. Normal permissions, such as ACCESS_NETWORK_STATE and INTERNET, were found in all the assessed monitoring apps.

Similarly, permissions like FOREGROUND_SERVICE, RECEIVE_BOOT_COMPLETED, and WAKE_LOCK were present in more than half of the apps. Others like ACCESS_WIFI_STATE, VIBRATE, SCHEDULE_EXACT_ALARM, USE_FINGERPRINT, CHANGE_WIFI_STATE, and USE_BIOMETRIC were found in less than half of the apps but were still present in multiple applications.

Table 2: Normal Permissions

Permission Name	Chat Tracker	Eyezy	Message and Call Tracker	Mobile Tracker	Desktime mobile time tracker	Employee time tracker (Apploye)	Track team manager	Quick books time tracking	Hubstaff time and hours tracker	Workganizer time tracking	Net monitor for employees	Chat message tracker remotely
ACCESS_NETWORK_STATE	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
ACCESS_WIFI_STATE	✔	✔				✔	✔	✔		✔		
FOREGROUND_SERVICE	✔	✔	✔	✔		✔	✔	✔	✔	✔		✔
INTERNET	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
RECEIVE_BOOT_COMPLETED	✔	✔	✔	✔		✔	✔	✔	✔	✔		
SCHEDULE_EXACT_ALARM	✔							✔				
USE_FULL_SCREEN_INTENT	✔									✔		
VIBRATE	✔	✔		✔				✔		✔		
WAKE_LOCK	✔	✔	✔	✔		✔	✔	✔	✔	✔		✔
QUERY_ALL_PACKAGES		✔										
USE_FINGERPRINT								✔		✔		
CHANGE_NETWORK_STATE						✔						
CHANGE_WIFI_STATE						✔	✔					
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS						✔						
ACCESS_NOTIFICATION_POLICY							✔					
USE_BIOMETRIC								✔		✔		
BLUETOOTH										✔		
MANAGE_OWN_CALLS										✔		
MODIFY_AUDIO_SETTINGS										✔		
READ_APP_BADGE										✔		

However, the assessment also revealed the presence of dangerous permissions across the apps. Dangerous permissions are a set of permissions in the Android operating system that grant apps access to sensitive user data or control over critical device functions. These permissions require explicit consent before they can be granted to an app. These permissions have the potential to pose risks to privacy and security if misused by malicious apps. Android prompts for permission to access certain permissions known as "dangerous" permissions. These permissions include access to call history, private messages, location, camera, microphone, and more. While these permissions aren't inherently dangerous, they could potentially be misused by harmful apps. That's why Android offers a choice to accept or decline these permissions, giving control over privacy and security.

The dangerous permissions found across the 12 assessed monitoring mobile applications as shown in Table 3 include:

1) READ_CONTACTS

This permission allows an app to read contact lists stored on devices. By granting this permission, the app can access information such as names, phone numbers, email addresses, and other details associated with contacts. Apps requesting this permission often need to display or interact with contacts, such as messaging apps, email clients, or social networking apps. This enables these apps to provide features like suggesting contacts for messaging, displaying contact information, or syncing contacts with other services [31]. Three (3) monitoring apps have required this permission.

2) WRITE_CONTACTS

This permission grants an application the ability to modify or update contact data. This permission allows apps to make changes to existing contacts or create new contacts on devices. However, it's essential to be aware of the potential risks associated with granting this permission. Misuse of this permission by a malicious app could result in unauthorized modifications to contacts, leading to unintended consequences. For instance, imagine if an app altered contact details for a trusted mortgage broker, replacing it with a fraudulent number and unknowingly calling the scammer instead, it could lead to the disclosure of sensitive financial information [31]. Only one (1) app requires this permission.

3) ACCESS_BACKGROUND_LOCATION

If an app requests permission to access a location in the background, it means it can retrieve device location information even when the app is not actively in use. However, it's important to note that requesting this permission does not automatically grant the app access to the location. Having this permission alone does not imply the app will track location without knowledge or consent. But, consider that granting this permission could potentially allow the app to continue tracking location even after closing it, which may raise privacy concerns [31]. This permission is required by only four (4) applications.

4) ACCESS_COARSE_LOCATION

Granting the app permission to access coarse location allows it to determine the approximate location based on the cell tower the device is connected to. This level of location accuracy is sufficient for emergency services to locate someone in case of an emergency. However, in most other cases, sharing this approximate location information may not be necessary or relevant to the app's functionality. Consider carefully whether the app genuinely requires access to a coarse location and whether the benefits of granting this permission outweigh any privacy concerns [31]. The majority (8) of the applications require this permission.

5) ACCESS_FINE_LOCATION

Granting the app permission to access precise locations allows it to utilize GPS and WiFi data to determine exact geographic coordinates. This level of accuracy can pinpoint location with high precision, potentially identifying the specific room or area within a building where located. Consider the implications of granting this permission, as it provides detailed information about whereabouts. Assess whether the app genuinely requires access to the precise location and weigh the potential benefits against any privacy concerns [31]. More than half (7) of the assessed applications require this permission.

6) CAMERA

By granting an app camera permission, it gains the ability to utilize camera hardware on devices. This allows the app to capture photos or record videos using the device's front or rear camera. Be cautious when granting this permission, as it gives the app the potential to access and capture visual information from surroundings. Ensure trust in the app and consider privacy preferences before allowing access to the device's camera [31]. Out of the 12 apps assessed, 3 require this permission.

7) RECORD_AUDIO

This permission enables an application to capture audio recordings and allows an app to record audio using the device's microphone. While this functionality is commonly used for legitimate purposes such as voice recording or audio communication, be cautious as it can also be potentially misused for eavesdropping or gathering sensitive information through sounds in the surrounding environment. Carefully consider the trustworthiness of the app before granting this permission [31]. Only 2 applications require this permission to function.

8) READ_EXTERNAL_STORAGE

Enables an application to access and read data from external storage. This permission allows the app to read files and data stored in external storage devices connected to the device, such as microSD cards or external hard drives. Granting this permission gives the app the ability to access and retrieve information from these external storage sources. Exercise caution and consider security implications before granting this permission, as it could potentially provide access to sensitive data stored in external storage devices [31]. Most applications do not require this permission as only 3 do.

9) WRITE_EXTERNAL_STORAGE

Enables an application to write to external storage. Granting this permission allows the app to write and modify data stored in external storage devices connected to the device. By allowing this permission, the app gains the ability to create, edit, and delete files in external storage sources, including microSD cards or external hard drives. Exercise caution and consider security implications before granting this permission, as it provides the app with control over data stored in external storage devices [31]. Five (5) out of 12 applications require this permission to function.

10) ACTIVITY_RECOGNITION

Enables an application to detect and identify physical activities. While this permission may appear innocuous, it becomes significant when combined with other location-related data. It is commonly utilized by activity tracking apps such as FitBit to monitor and analyze physical movements. However, when paired with additional location information, this permission has the potential to reveal detailed insights into user's activities and their specific locations. Consider the implications of granting this permission and the potential for privacy concerns [31]. Only 2 applications require this permission.

11) CALL_PHONE

Enables an application to make a phone call directly, bypassing the user interface for confirmation. This permission allows the app to initiate phone calls without knowledge or consent, which could result in unauthorized calls and potential unexpected charges or fraudulent activities. Be cautious when granting this permission and carefully review the app's trustworthiness before allowing it to make calls on behalf [31]. Only 1 monitoring application requires this permission.

12) SYSTEM_ALERT_WINDOW

Allows an application to create windows that are shown on top of all other applications. App permission grants the app the ability to overlay windows or pop-up notifications on top of other apps, even when they are in use. While this can be useful for certain system-level functionalities or floating widgets, it also presents a potential risk for intrusive or malicious behaviour. Apps with this permission could display unwanted or deceptive content, disrupt user experience, or potentially capture sensitive information [31]. Only 2 applications require this permission.

Table 3: Dangerous Permissions

Permission Name	Chat Tracker	Eyezy	Message and Call Tracker	Mobile Tracker	Desktime mobile time tracker	Employee time tracker (Apploye)	Track team manager	Quick books time tracking	Hubstaff time and hours tracker	Workganizer time tracking	Net monitor for employees	Chat message tracker remotely
READ_CONTACTS	✔	✔								✔		
WRITE_CONTACTS	✔											
ACCESS_BACKGROUND_LOCATION				✔		✔		✔	✔			
ACCESS_COARSE_LOCATION		✔	✔	✔		✔	✔		✔	✔		✔
ACCESS_FINE_LOCATION		✔		✔		✔	✔	✔	✔	✔		
CAMERA		✔						✔		✔		
READ_PHONE_STATE		✔						✔				
RECORD_AUDIO		✔								✔		
READ EXTERNAL STORAGE					✔			✔		✔		
WRITE EXTERNAL STORAGE					✔	✔		✔		✔	✔	
ACTIVITY RECOGNITION								✔	✔			
CALL PHONE								✔				
SYSTEM_ALERT_WINDOW						✔				✔		

5.2 Comparative analysis of the dangerous permissions across the assessed applications

Figure 1 illustrates the graphical representation depicting the frequency of dangerous permissions identified across various scanned applications. Notably, QuickBooks and Workanizer Time Trackers exhibit the highest incidence of dangerous permissions, each encompassing 8 out of the 12 identified. Conversely, Chat Message Tracker, Net Monitor for Employees, and Message and Call Trackers demonstrate the lowest occurrence of dangerous permissions, each possessing only 1 out of the 12 identified. Eyezy manifests 50% of the identified hazardous permissions, while the remaining evaluated applications exhibit less than 50% of these permissions.

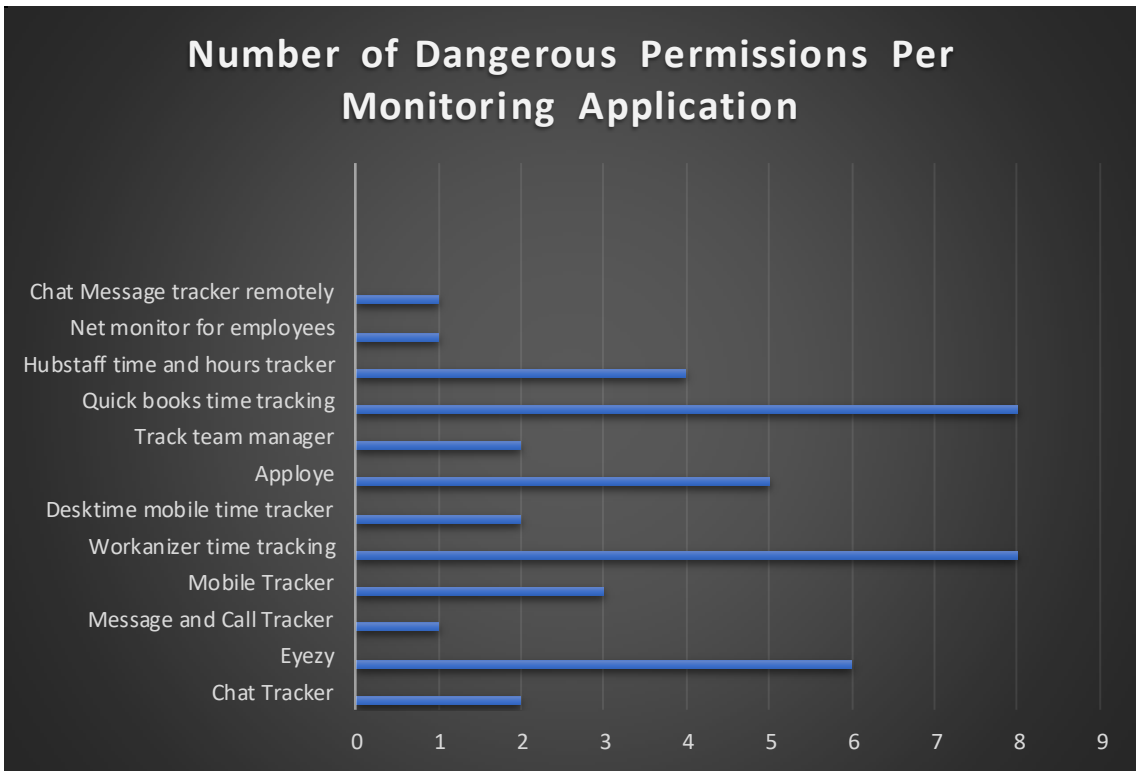

Figure 1: Comparison of identified dangerous permissions amongst the assessed monitoring Apps

6. Discussion

In the following sections, we will delve into the outcomes obtained from our analysis of monitoring mobile applications. This discussion focuses on two main aspects: the significant consequences of privacy policies and the complex matter of permissions, specifically those that could potentially pose risks, concerning the privacy of remote employees. This exploration aims to highlight the essential insights derived from our assessment, shedding light on the crucial points where organizational practices meet individual privacy rights within the context of remote work.

6.1 Implications of Monitoring Mobile Applications Having Dangerous Permissions

The operation of monitoring apps is contingent upon acquiring specific permissions, a process with both potential advantages and concerning implications. Permissions such as READ_PHONE_STATE, ACTIVITY RECOGNITION, and SYSTEM_ALERT_WINDOW are essential for monitoring app functionality, enabling seamless remote tracking of employees. However, the discussion becomes more intricate when we delve into permissions that grant access to sensitive employee data.

Consider the necessity of location monitoring. Access to an employee's location is vital to ascertain work-related engagements. Permissions like ACCESS_COARSE_LOCATION achieve this by providing an approximate location through the nearest cell tower. However, the story becomes more intricate with permissions like ACCESS_BACKGROUND_LOCATION and ACCESS_FINE_LOCATION, which offer more detailed location data. While these permissions may have specific applications, they simultaneously raise privacy concerns by potentially infringing upon an individual's private space.

A key consideration is that monitoring apps are typically installed on employees' mobile devices, distinct from organization-provided devices. This distinction is crucial, as continuous data gathering about an employee's location, even outside of work hours, encroaches upon their privacy. Unlike work-confined laptops or desktops, personal mobile devices are a constant presence in individuals' personal lives, making their ongoing monitoring an intrusive practice.

The quest for comprehensive monitoring necessitates permissions like READ_CONTACTS and READ_EXTERNAL_STORAGE, fundamental for tracking messages and calls. However, these permissions also access personal data, raising questions about the boundaries of user privacy. The situation becomes murkier with permissions like WRITE_CONTACTS and WRITE_EXTERNAL_STORAGE, which imply the capacity to modify an employee's contacts and files. While such permissions might be justified for organization-managed devices, their intrusion into personal mobile devices' domain prompts ethical inquiries.

Furthermore, CAMERA and RECORD_AUDIO permissions, ostensibly critical for monitoring app operation, present potential privacy challenges. With many remote workers setting up their workstations at home, visual and audio recordings might inadvertently capture sensitive information or discussions involving household members. This dual

privacy infringement, affecting both the employee and their cohabitants, underscores the need for cautious handling of these permissions.

The gravity of these permissions is undeniable; they underpin the distinct functionality of monitoring apps. However, their utilization necessitates a nuanced equilibrium between operational efficiency and user privacy. While these permissions are vital for app effectiveness, they also harbour cybersecurity implications. For instance, permissions like CALL_PHONE, enabling the app to place calls without user consent, introduce significant cybersecurity vulnerabilities, potentially facilitating unauthorized usage.

In essence, the journey of monitoring apps through the permissions landscape is a complex endeavour. Navigating the delicate balance between app efficacy, user privacy, and cybersecurity presents a substantial challenge. The intricate interplay of these factors shapes the ethical and practical dimensions surrounding the integration of monitoring apps in the dynamic landscape of remote work.

6.2 Implications of the Absence of Privacy Policy

The findings highlight a significant aspect: monitoring apps necessitate multiple permissions, enabling the acquisition of sensitive employee data. This strategic data collection empowers employers to cultivate trust in employee engagement and productivity. However, despite these permissions, a noteworthy omission prevails across all assessed monitoring apps – the lack of provisions for addressing employees' privacy concerns. This absence of privacy policies underscores a critical gap, as privacy policies are crucial instruments for safeguarding employee rights and organizational transparency.

Privacy policies assume a pivotal role in addressing these concerns. They serve as a conduit for transparency, granting users insights into the data collection process. These policies illuminate the purposes behind data collection, delineate storage methods, outline security measures, and address potential sharing arrangements with third parties. By offering comprehensive clarity, privacy policies serve as a foundational pillar in building trust between entities and users. They are instrumental in conveying how personal data is managed and contribute to the establishment of ethical data practices.

These policies extend their coverage to various dimensions. Notably, they encompass data retention periods, elucidate protocols for data sharing, delve into the utilization of cookies and tracking technologies, and articulate user entitlements in relation to their data. Moreover, privacy policies provide individuals with clear channels through which they can engage with organizations regarding privacy inquiries or requests. Mandated by legal frameworks like the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, privacy policies are typically readily accessible to users through a website or app's footer. In many cases, users are required to acknowledge and accept the terms of the privacy policy before utilizing the service.

By proactively embracing privacy policies, organizations not only adhere to legal obligations but also manifest their commitment to respecting user privacy. Such proactive measures bolster organizational credibility, promote responsible data management, and facilitate users in making informed decisions about sharing their data. As privacy becomes an increasingly significant concern in the digital landscape, privacy policies emerge as an essential safeguard, ensuring that the delicate balance between data utilization and user privacy is maintained with utmost diligence and care. The absence of a privacy policy can have profound implications, presenting several potential pitfalls for both organizations and individuals.

1) Lack of Transparency

Without a privacy policy, there is no formal mechanism for disclosing how personal information is collected, utilized, and shared. This absence of transparency can erode trust and leave individuals in the dark about how their data is handled.

2) Legal Non-Compliance

In jurisdictions with privacy regulations, the absence of a privacy policy can lead to legal non-compliance. This can result in legal penalties, fines, and damage to an organization's reputation.

3) Undefined User Consent

Without a privacy policy, organizations may not adequately inform users about the data collection and processing practices. This lack of information denies users the opportunity to provide informed consent, potentially leading to misunderstandings and distrust.

4) Inadequate Data Protection

A missing privacy policy could mean that data protection measures are not clearly outlined. This could result in inadequate safeguards against data breaches and unauthorized access.

5) Undisclosed User Rights

Users may be unaware of their rights concerning their personal data if a privacy policy is absent. This can hinder individuals from exercising control over their data and making informed choices.

6) Compromised Trust and Reputation

Organizations without privacy policies may struggle to establish trust with users. The absence of a commitment to data protection can tarnish an organization's reputation and hinder customer loyalty.

7) Limited Guidance

A privacy policy serves as a guide for employees and users on data handling practices. Without this guidance, individuals may be unsure about the appropriate ways to manage data, potentially leading to mishandling or breaches.

8) Missed Business Opportunities

In some cases, the lack of a privacy policy may deter potential customers or business partners who value transparency and data protection.

Overall, not having a privacy policy can expose organizations to legal risks, damage their reputation, and hinder their ability to foster trust with customers. It can also leave individuals without clear guidance on how their data is used and their rights regarding their personal information.

7. Conclusion

Remote work is here to stay as most employees are reluctant to return to the office full-time. In organizations dealing with sensitive information and confidential matters, heightened security measures are often implemented to safeguard trade secrets and internal strategies. However, these measures can sometimes encroach upon employee privacy, leaving employees feeling as though their privacy is compromised within the workplace. On the other hand, some companies prioritize employee privacy at the expense of employer security. Striking the right balance requires conducting thorough research and communicating managerial expectations to create a harmonious environment.

Monitoring apps should include only permissions that are necessary to achieve their goals and try as much as possible to avoid the use of permissions that violate employees' privacy. All monitoring apps should have a privacy policy that provides the employee with enough information on how their sensitive data are collected and used.
In light of the ongoing trend towards remote work and the inherent challenges surrounding employee privacy and organizational security, future research should focus on developing guidelines and best practices for the responsible implementation of monitoring applications in remote work settings. This research could delve into the identification of essential permissions required for monitoring applications to fulfil their intended purposes effectively while respecting employee privacy rights. Additionally, further exploration is warranted into the formulation of comprehensive privacy policies for monitoring apps, ensuring that employees are adequately informed about the collection and utilization of their sensitive data. Moreover, future work could entail the development of technological solutions or frameworks that strike a delicate balance between organizational security imperatives and employee privacy concerns, fostering a conducive and equitable work environment for remote employees. By addressing these critical areas, organizations can better navigate the complexities of remote work while upholding both security standards and privacy rights.

Data Availability
All reports of the security assessments of the applications are available on request.

Conflict of Interest
The authors declare that there is no conflict of interest with anyone for publication of this work.

Funding Source
None

Authors' Contributions
Author-1 Explored existing scholarly works, formulated the research design, and authored the conclusive version of the manuscript.

Author-2 Conducted the experimental procedure and delivered the findings alongside an initial framework of the manuscript.

All authors critically examined and revised the manuscript, providing edits and ultimately endorsing the final iteration of the document.

Acknowledgements
We extend our heartfelt gratitude to God Almighty for the profound insight and inspiration that guided our work. Additionally, we would like to express our appreciation to the International Journal of Scientific Research in Computer Science and Engineering for their invaluable review and constructive suggestions, all of which have been instrumental in enhancing the clarity and visibility of our research endeavour.

References

[1] P. V. Falade, "Analysis of 419 Scams : The Trends and New Variants in Emerging Types," vol. 11, no. 5, pp. 60–74, 2023.
[2] S. S. -, "Design and Implementation of Chatbot using Python," *Int. J. Multidiscip. Res.*, vol. 5, no. 6, pp. 13–18, 2023, doi: 10.36948/ijfmr.2023.v05i06.9993.
[3] R. C. Jalagat and A. M. Jalagat, "RATIONALIZING REMOTE WORKING CONCEPT AND ITS IMPLICATIONS," no. April, 2019.
[4] S. Trivedi and N. Patel, "Virtual Employee Monitoring: A Review on Tools, Opportunities, Challenges, and Decision Factors," *Empir. Quests Manag. Essences*, vol. 1, no. 1, pp. 86–99, 2021, [Online].
[5] S. E. Chang, A. Liu, and S. Lin, "Exploring privacy and trust for employee monitoring," *Ind. Manag. Data Syst.*, vol. 115, pp. 88–106, Feb. 2015, doi: 10.1108/IMDS-07-2014-0197.
[6] D. J. Borkovich and R. J. Skovira, "Working From Home : Cybersecurity in the Age of Covid-19," no. September, 2020, doi: 10.48009/4.
[7] O. Karpenko, A. Kuczabski, and V. Havryliak, "Mechanisms for providing cybersecurity during the COVID-19 pandemic : Perspectives for Ukraine," March 2021.
[8] S. Vicaria, "The Rise Of Remote Work And How To Handle A Remote-First Team," 2023.
[9] G. Crossland, A. Ertan, and N. M. Anima, "Remote Working and Cyber Security," no. January, pp. 1–27, 2021.
[10] A. M. Jalagat, "Rationalizing Remote Working Concept and," *Glob. J. Adv. Res.*, no. 3, pp. 95–100, 2019.
[11] J. R. C. Nurse, N. Williams, E. Collins, N. Panteli, J. Blythe, and B. Koppelman, "Remote Working Pre- and Post-COVID-19 : An Analysis of New Threats and Risks to Security and Privacy," pp.1–8.
[12] L. Atstāja, D. Rūtītis, S. Deruma, and E. Aksjoņenko, "Cyber Security Risks And Challenges In Remote Work Under The Covid-19 Pandemic," no. January 2022, pp. 12–22, 2021, doi: 10.15405/epsbs.2021.12.04.2.
[13] K. Okereafor, *Cybersecurity in the COVID-19 Pandemic*, no. March. 2021. doi: 10.1201/9781003104124.
[14] M. Burrows, D. Hadzic, KPMG Internacional, and K. Stoltz, "Current trends in remote working," *KPMG Glob.*, pp. 2–17, 2022,

[Online].
[15] I. Aldasoro, J. Frost, and L. Gambacorta, "Covid-19 and cyber risk in the Financial sector," no. 37, 2021.
[16] B. Obada-obieh, Y. Huang, K. Beznosov, and K. Beznosov, "Challenges and Threats of Mass Telecommuting : A Qualitative Study of Workers This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security .," 2021.
[17] B. J. Arnold, C. Kou, and C. Oates, "Cyber Security and Privacy risks in a remote work environment," 2020.
[18] M. K. Pratt, "Remote work cybersecurity: 12 risks and how to prevent them," 2022.
[19] K. J. Rotenberg, "Trust in the Workplace," *Psychol. Interpers. Trust*, no. June, pp. 92–101, 2019, doi: 10.4324/9781351035743-9.
[20] S. K. Parker, C. Knight, and A. Keller, "Remote Managers Are Having Trust Issues," 2020.
[21] D. Zielinski, "Monitoring Remote Workers," 2020.
[22] A. Dimitropoulou, "Remote Work and its effects on Work-Life Balance," 2023.
[23] P. V Falade and G. B. Ogundele, "Vulnerability Analysis of Digital Banks ' Mobile Applications," vol. 1, no. 1, pp. 44–55, 2022.
[24] C. Hawes, "What is mobile app monitoring? And the importance of mobile analytics," 2022.
[25] E. Czerwonka, "How do companies track employees?" 2023.
[26] Immuniweb, "Immuniweb AI for Application Security," 2022.
[27] ImmuniWeb, "ImmuniWeb AI for Application Security," 2023.
[28] C. Kumar, "12 Mobile App Scanner to Find Security Vulnerabilities," 2022.
[29] SoftwareTestingHelp, "10 Best Mobile APP Security Testing Tools In 2022," 2022.
[30] Iubenda, "What is a Privacy Policy?," 2023.
[31] G. McDowell, "30 App Permissions To Avoid On Android," 2020.

AUTHORS PROFILE

Polra Victor Falade holds a B.Tech in Computer Science with a specialization in Cyber Security, which I earned from the Federal University of Technology Minna, Niger State, Nigeria in 2016. Subsequently, pursued an MSc in Information Security from the University of Surrey, UK, graduating in 2021. These educational experiences have equipped her with a comprehensive understanding of cybersecurity principles and best practices. Currently, she is serving as an Assistant Lecturer in the Department of Cyber Security at the Nigerian Defence Academy (NDA) in Kaduna, Nigeria. In this role, she has been actively involved in educating future cybersecurity professionals, fostering a culture of cybersecurity awareness, and conducting research in the field. Her commitment to academic excellence is reflected in her continuous pursuit of knowledge and my dedication to her students. Furthermore, she is a professional member of the Cyber Security Expert Association of Nigeria (CSEAN), which has provided me with valuable networking opportunities and a platform to stay updated with the latest developments in the cybersecurity domain. Also, a member of Internet Society, Nigeria Chapter. Her primary passion lies in research and academic writing, particularly in the areas of Information Security, AI Security, Privacy and cybersecurity-related research.

Patience Ocheche Momoh, holder of a Postgraduate Diploma in Cybersecurity from The Nigerian Defence Academy since 2023, presently serves as a Project Manager Assistant within the Project Management Department at Access Solutions Limited, Abuja. With a strong inclination towards technology and a fervent interest in cybersecurity, she is pursuing additional studies in Digital Forensics intending to become a Digital Forensics Examiner. Additionally, she possesses expertise in UI/UX design and extensive knowledge of Quality Assurance.

