INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Electronic Finance

ISSN online: 1746-0077 - ISSN print: 1746-0069
https://www.inderscience.com/ijef

Growth of mobile applications and the rise of privacy issues

Ayush Goel, Gurudev Sahil

DOI: 10.1504/IJEF.2024.10054417

Article History:

Received:	16 December 2022
Last revised:	10 January 2023
Accepted:	27 January 2023
Published online:	01 December 2023

Growth of mobile applications and the rise of privacy issues

Ayush Goel and Gurudev Sahil*

CHRIST (Deemed to be University),
Pune, Lavasa Campus, 412112, India
Email: ayush.goel@res.christuniversity.in
Email: gurudev.sahil@christuniversity.in
*Corresponding author

Abstract: Mobile apps are used by more and more internet users for daily chores, but processing personal data with them poses a major security risk. The wide range of data and sensors in mobile devices, the use of different types of identifiers and the increased ability to monitor consumers, the complex mobile application ecosystem and application developer limitations, and the extensive use of third-party technologies and services, are the main risks. Privacy concerns extend beyond mobile users. Corporate executives need fast, global access to their database. White goods/smart building equipment suppliers offer mobile apps for remote use. This research study will integrate these concerns. Due to these factors, smartphone applications have struggled to enforce the General Data Protection Regulation's (GDPR) data protection rules. Mobile app designers and service providers may struggle to meet GDPR rules for data disclosure and permission, data protection by design and default, and operational secrecy.

Keywords: privacy of data; confidentiality in mobile applications; websites; Amazon; GDPR; application; aggregators.

Reference to this paper should be made as follows: Goel, A. and Sahil, G. (2024) 'Growth of mobile applications and the rise of privacy issues', *Int. J. Electronic Finance*, Vol. 13, No. 1, pp.20–35.

Biographical notes: Ayush Goel is currently pursuing Full-Time PhD from CHRIST (Deemed to be University), India. He has completed his Master's LLM in Corporate and Commercial Laws from CHRIST (Deemed to be University), Bangalore. Currently, he is working on product liability and data confidentiality issues faced by intermediaries.

Gurudev Sahil is an Assistant Professor at CHRIST (Deemed to be University), India. He has been a legal associate for five years in Law Remedium. He has completed his PhD in law from Law College, Bhagalpur and his master's LLM in Criminal and Corporate Law from Indian Law Institute, Delhi. Currently, he is teaching Space Law, Commercial Arbitration, and Company Law at CHRIST (Deemed to be University), India. In general, he has published six research papers.

1 Introduction

Smartphones are arguably the most indispensable gadgets, as mobile apps have become an integral part of everyday life. Almost everyone, from young children to older adults, uses smartphones extensively in all aspects of their lives. Smartphones have begun to dominate people's digital habits due to the development of mobile technology, mobile access to high-speed internet, and the interactivity of smartphone user interfaces. People spend a lot of time using mobile applications as they serve many different functions, from communication to entertainment (Reychav et al., 2019). It can indeed be said that the development of smartphone applications is one of the most productive sectors. Millions of new applications are released yearly, allowing individuals to have more fun, connect with others, and increase productivity and creativity. "In the United States, people spend an average of 3.5 hours per day using their mobile phones, with 90% of smartphone internet use and 77% of tablet use using mobile apps" (Wurmser, 2018). "Every day, app stores offer many new mobile apps that cater to customers' online selling, gaming, and financial management needs" (Balapour et al., 2019). "According to a study, from the third quarter of 2016 to the first quarter of 2018, the average number of mobile applications available through the Google Play Store per day was around 6,140" (Ceci, 2022).

By keeping our phones close to us and spending a lot of time in apps and services, apps can collect and process much personal and sensitive information. Apps can compromise individual privacy in many ways, even when we voluntarily share and contribute some of this knowledge. "However, despite the high statistics, the majority of people in the United States are still reluctant to download mobile apps, and it turns out that the average number of downloads per month is zero" (Perez, 2017). "Other studies have shown that after three months, the majority of users (80%) no longer use the mobile apps they downloaded" (Hopwood, 2017).

The growth of mobile applications is unstoppable. As we have discussed above, at present, for each and everything, we have a mobile application that eases our day-to-day life; for example, for daily groceries, we have a mobile application like Blinkit or Big basket where the user can get groceries within 30 minutes at their doorstep. There is many more such application for various works. No doubt these mobile applications are providing easement to us, but they are also creating a lot of privacy issues. Individuals are constantly forced to choose between data privacy and the availability of smartphone programs; in many cases, they don't even realise they're making a choice. While regulations and procedures are in place, and Europe's General Data Protection Regulation (GDPR) is doing the trick, there are still many risks. Protecting personal information is a fundamental right, and many different approaches have been proposed and put into practice to ensure this right is respected.

On the other hand, there are some inconsistencies between the law and how it effectively translates into technical issues. Moreover, the average consumer and the engineers have enough knowledge and understanding to make the right decision. The present paper will us on the privacy issue faced by individuals as well as how GDPR is working on these issues and how they are still lack. Following a theoretical approach, we conduct an exploratory study to understand common practices and barriers in mobile application development. The overall goal of our research is to gain this knowledge. The researcher will collate present and near-future challenges/issues related to privacy posed

by these mobile applications. Further, it will also include the various measures taken to tackle privacy issues. Although the study pertains to the Indian environment, a better understanding of GDPR is referred to.

2 Evolution of mobile application

A mobile application, sometimes known as a mobile app, is a software developed specifically for mobile platforms. Developments in current communication technology capabilities appear to be responsible for this finding. Integrating multimedia with IT, web, and cutting-edge technologies leads to the development of new applications. In particular, mobile communications have been a research focus (yes) for quite some time for mobile device manufacturers, mobile service providers, application developers, and numerous other researchers in the fields of information technology (IT) and information systems (Carey, 2022). "While Apple's launch of the iPhone is considered the start of the mobile app space, its phenomenal growth may be due to the entry of several new competitors, most notably Motorola, LG, and Samsung" (Rakestraw et al., n.d.). As a result of this competition, a whole new product category—the smartphone—was born. Because of their ability to run mobile applications, smartphones offer a wider range of functionality than standard cell phones. With the help of these programs, smartphones can now send and receive e-mail, play music, movies, and video games, and even remotely talk to computers in almost any location on the planet (Coustan et al., n.d.).

PCs and smartphones share a lot of hardware, consisting of many individual components. Every smartphone contains a processor, a stick of RAM (or memory stick), a display adapter, USB ports, and internal storage. Individuals can also personalise and modify their devices to meet specific requirements. For example, to play games, a user may wish to purchase a smartphone with a multi-core processor and enough internal storage to accommodate the largest games. Most modern smartphones are equipped with touchscreens, eliminating the need for traditional keyboards. Also, buy USB accessories for your phone, such as headsets and data transfer cables (Coustan et al., n.d.).

Mobile apps have grown to the point where they are now an integral part of our daily lives. These apps now provide solutions to all of our needs, from the most trivial to the most important, including the ability to order food delivery, play games, buy clothes and other goods, and keep in touch with loved ones who live in different parts of the world. We spend over 80% of our waking hours using our mobile apps. But where did it start, and how did it develop into the cutting-edge technology readily available today?

IBM first introduced SIMON in 1993. A smartphone with a touchscreen interface and built-in applications and e-mail capabilities, such as a "calendar, address book, world clock, calculator, notepad, games, and fax" (AppVerticals, 2020).

It wasn't until 2002 that RIM released the first BLACKBERRY—a device that could receive and send e-mail wirelessly. When Apple introduced the world's first iPhone in 2007, it could only run the company's pre-installed mobile apps (namely 'maps, photos, text, and weather') (AppVerticals, 2020).

2008 was the year Apple first offered the iPhone 3G and 552 different apps through its App Store (AppVerticals, 2020). Google powers both the Android operating system and the Android Market. HTC released the first Linux-based Android smartphone for the Android market (AppVerticals, 2020).

An app distribution service called Blackberry world launched in 2010. Apple's first-generation iPad came with 3,000 pre-installed apps (AppVerticals, 2020). In 2011, APP was awarded Word of the Year for its achievements 2010. Decided to build an Amazon app store for Android. One million mobile applications have been fully created. An Android app dubbed 'Beautiful Widget' became the first paid app to hit 10 billion downloads (AppVerticals, 2020).

The App Store was formerly the Google Play Store and was renamed GOOGLE PLAY in 2012. There have been over 15 billion app downloads from Google Play. In 2016, Chrome OS gained support for the Google Play Store and its associated apps. At its annual I/O developer conference, Google unveiled Instant Apps for the first time. Google has added a new section, 'Free App of the Week', which features a free app each week. (AppVerticals, 2020).

"Huawei's operating system, Harmony OS, will be released sometime in 2019. The number of app downloads in the app store reached a new high, reaching 204 billion times. In 2019, TikTok became a mobile app phenomenon, generating $177 million in revenue. The Disney+ streaming service quickly became the second most popular app of 2019, bringing in $50 million in initial revenue within its first month of being available to users" (AppVerticals, 2020). With the evolution comes the threat of data protection and privacy. Most mobile app developers built heavy firewalls or authorisation matrices to tackle this issue. At the same time, these strategies helped in data protection but created a bad user experience.

Further, these strategies were ineffective as far as privacy concerns. Machine learning techniques can curve this gap, and it is gaining momentum and is expected to increase soon. One must be cautioned that machine learning has its issues as far as privacy is concerned. Hence, the benefits vs. challenges need to be evaluated.

2.1 Downfall of internet website against mobile application

It can be said that the application has suppressed internet websites. Thanks to advancements in technology, online developers are now able to program not only traditional web browsing but also browsing on mobile devices. The shift to using mobile apps instead of websites will only increase for some reasons. The first advantage is that the mobile app can be used almost anywhere, whether or not you have access to a wireless network or have access to particularly large or expensive hardware. Additionally, many businesses and other website owners have developed mobile versions of their websites to provide faster download speeds. These mobile versions also feature an optimised user interface and other elements that add to the functionality of mobile browsers (Rakestraw et al., n.d.).

2.2 Transformational rise of mobile application

Smartphone nodes have been accessing internet content through their mobile devices since 3G, and 4G digital networks were introduced. The accessibility of social media has quickly turned the smartphone into a very useful device. Mobile marketing emerged as a direct result of the increase in smartphone users. Mobile marketing makes connecting with customers easy. Apps are compatible with various operating systems, including Android, Symbian, and iOS. Smartphone advertising utilises many applications to its advantage (Keeton and Wei, 2021). Marketing professionals quickly saw the potential of

mobile devices as a widely used distribution channel and scrambled to capitalise on the trend (Deshwal, 2016). Thanks to mobile portals, many marketers can reach end customers at a much lower price than traditional marketing promotions and build great relationships with users. Because advertisers can now personalise messages – also known as 'customisation' – their interactions with customers become more engaging. Customers are singled out by their name and address, location, buying habits, and social and communication preferences (Deshwal, 2016). These applications have bridged the time and place gap and brought many advantages on a managerial, societal, and theoretical basis. Some of these are saving productive time, including a larger population, higher reach factor even in remote places and villages, more employment opportunities, and tracking workflow/process improvement methods.

3 Development of mobile application in India

"According to a 2019 report by the Progressive Policy Institute, India is considered one of the major tech-centric countries in the world and is expected to overtake the US as the largest developer population center by 2024" (Mandel and Long, 2019). The above data shows that India has the highest number of mobile app downloads, as the country has more than 500 million mobile app users. This provides enough data to understand the current state of app development and manufacturing in India. It cannot be denied that India has made huge strides in app development; it is an irrefutable fact. "In recent years, the number of apps built by Indian app developers and housed in Google Play Store and Apple App Store has increased" (Subramaniam, 2022).

3.1 Fifth-generation wireless cellular network

With its cutting-edge radio technology, 5G wireless cellular networks are poised to revolutionise the telecommunications industry. It's not a more advanced form of 4G; rather, it's a completely different technology that's worth discussing in our time.

Industry experts predict it will do more than simply dramatically improve internet connectivity. Since 5G provides a unified network structure, network devices for collecting and sharing information in real-time will become less cumbersome and more useful.

As we've seen, the mobile device industry is primed for the disruption 5G will bring. Moreover, it is also poised to have a major impact on mobile application development. Improved speeds and more advanced features are just the beginning of what 5G promises to revolutionise the user experience.

"Users of 5G-enabled mobile apps will have access to cutting-edge innovations such as the Internet of Things (IoT), ultra-high-definition movies, cloud computing, augmented and virtual reality (AR & VR), and more" (Patrick, 2021) It's official: mobile app development will be profoundly transformed by 5G. In simple terms, it can be said that with 5G connectivity, the individual can access the internet at a greater speed. The buffering time for highly defined videos and movies will be very minute, and the applications like virtual reality will work more effectively as the connectivity speed will be high.

Since 5G is about a hundred times faster than 4G, it will soon surpass LTE in terms of speed. LTE is the fastest mobile technology available today. It can transfer data at a maximum rate of 300 megabits per second (Mbps), a very high number.

"According to recent research results, 5G can transmit up to 3 gigabits per second (Gbps) of data. In the future, this speed is expected to increase by a factor of 20, reaching speeds of 10 gigabits per second" (Patrick, 2021). Thus, users can upload and download files quickly, enhancing the program's utility. "5G can send and receive data in fractions of a second because it uses ultra-reliable low-latency communications (URLLC). Mobile apps can provide real-time data if the connection is minimally disruptive. Typical latency observed on 4G networks is 50ms; however, latency across 5G networks is much lower" (Patrick, 2021). Up to one million devices can connect to the 5G network simultaneously. Increased connection density will allow IoT integration into mobile applications to run more smoothly. "This feature bypasses the limitation of 4G, which can only connect 2,000 gadgets simultaneously within a radius of 0.38 square miles. Its improved features allow programs and hardware to communicate with each other smoothly, even when dealing with heavy network traffic" (Patrick, 2021).

In order to provide superior connectivity, 5G technology is being developed to function in different frequency band ranges. "All smartphone apps will work on all frequency bands, including the low band (sub-1 GHz), mid-band (1 GHz to 6 GHz) used by LTE, and the high band consisting of millimeter waves (millimeter waves)" (Patrick, 2021).

3.2 Applications designed for wearable technology

Wearable devices, including smartwatches, body monitoring devices, etc., are now catering to the application development field, which was previously limited to smartphones and tablets. These devices are often used to assist patients and medical staff. Under no circumstances should we underestimate the importance of the agriculture and healthcare industries (Insights Success, 2021). As a broad term, 'wearable app development' refers to making apps for wearable devices like smartwatches, fitness bands, and immersive virtual reality glasses. Developing applications for wearable devices should focus on creating software that is not only useful but also easy to operate. This should be done keeping in mind wearable devices' constrained space and resources. When building an application for wearable technology, you need to consider many considerations, including the type of wearable device you intend to support, interface design, and overall user experience.

- Some of the benefits are: fitness and health tracking, heartbeat, steps taken, and calories burned are all things fitness trackers can monitor. Individuals trying to improve their health or maintain their fitness levels will find this material helpful. In addition, sleep tracking is also possible using wearable technology. People who have difficulty sleeping or wish to monitor sleep quality may find the published evidence helpful. Third, there are smart devices that measure blood pressure along with other health indicators. Wearable technology can also aid in overall weight loss by recording the amount of food consumed versus the number of calories burned.

- Productivity: smart wearables for entertainment and social networking are already popular; nevertheless, these gadgets have great potential to drive growth. Because they don't require the user to use their hands, many types of wearable technology can be used even when the user is engaged in other activities. This paves the way for developing new classes of applications that can take advantage of the unique capabilities of wearable technology.
- The functionality of the GPS: An increasing number of wearable devices are equipped to use GPS. This information can be used to create applications that take advantage of the user's location. This is great for health and fitness apps that track user progress and provide encouragement. Among other things, it can navigate or locate nearby goods and businesses. Additionally, the capabilities of GPS can be combined with other sensors to provide users with specific information about their environment.

3.3 Internet of Things

There is a general understanding of the need for everyday gadgets to become increasingly intelligent, although many may not officially recognise the IoT (Insights Success, 2021). "From a developer perspective, our goal was to make an app that would assist with existing forms of home automation, such as the management of audio equipment, video equipment, climate control, etc." (Gillis, n.d.). See the development of applications that have the function of operating factories, offices, and even automobile machines. Previously, apps were only developed for home and entertainment purposes, but now we see more and more apps being developed with such controls. Providing mobile applications that take advantage of the IoT will inevitably become more commonplace in the coming years (Tikku and Singh, 2022).

3.4 Application related to cloud-based

To ensure a seamless experience across all user devices, modern applications and services typically do not save user data locally but in remote, cloud-based servers (Yan et al., 2017). Priorities for customers when purchasing a smartphone include portability (the ability to use the device on other platforms), security (the ability to prevent unauthorised access to data), data storage (the ability to retain data for future use), and data processing (the ability to derive knowledge or insight from data). Since most customer information is now stored in the cloud, users can access their files regardless of the type of device they use to launch the application (Menon, 2019). This is a huge improvement over older applications, where application developers are now focused on creating programs that can take advantage of cloud services.

4 Case studies on mobile application marketing

With time the development of mobile applications has increased a lot. It is observed that now every business has its application. Even the businesses before their website are now shifting and working on their mobile applications. But businesses must understand that to

be in the business, they should be creative and unique with their applications. Some of the examples are:

4.1 KLM airlines application

Well, we all know that KLM has the biggest airplane fleet. They have been operating for a long time. With time KLM airlines have also come up with its mobile application. To grow their application, they have done a lot of work. To grow their application usage through mobile, they have played a very good game. KLM Airlines' main goal has been encouraging passengers to use their mobile devices for flight bookings. Another reason for developing this mobile app was to provide the basis for other mobile marketing strategies, such as mobile passbooks and destination reminders. "The only way to achieve this is to convince more customers to use the mobile app" (Sharma, 2021).

"KLM is running a promotion where anyone using its mobile booking engine will get free access to the app for three weeks. Users can access it using mobile vouchers stored in Passbook (for iPhones) or Google Wallet (for Android phones). They received a notification based on their location reminding them to redeem their discount at a nearby KLM lounge. A 34% increase in bookings and a 38% increase in mobile revenue resulted in a 17% increase in KLM airline mobile site traffic" (Yehoshua, 2016).

4.2 Amazon shopping application

Amazon, the world's largest online retailer, has developed a dedicated marketplace to distribute mobile applications for the Android platform. The marketplace will also serve as the main user interface for Amazon's Kindle Fire, which runs on a custom version of the Android operating system. The alternative to the normal Android Market is designed to be more streamlined, user-friendly, and intuitive than the original Android Market and accessible to everyone using Android.

The success of their new strategy may be largely due to the enhancement of their keywords. "They found that simply using the word "shopping" in the app's title was extremely beneficial to their marketing efforts. Only 2.12% of people who searched for the term found their app before they added the word "shopping" to the title. Adding the word "shopping" almost quadrupled the traffic, bringing the total to 9.88% of global traffic" (Sharma, 2021).

4.3 British supermarket chain – ASDA application

British Supermarket Chain is one the biggest grocery stores in the UK. With time British Supermarket Chain upgraded itself with its application called ASDA. ASDA intends to use technology to develop an app that will make online shopping easier for individuals, especially for people with many things going on in their lives simultaneously, such as busy mothers. They want the app to be responsible for 10% of all transactions done with online grocery shopping (Sharma, 2021).

Before developing the app, the company surveyed its existing customers to identify the most important app features that would simplify their shopping experience. They kept the app design simple and clear in response to user comments and suggestions to make it as user-friendly as possible for people from all walks of life (Talking Retail, 2013).

They often show people what they buy, using reminders like "Did you forget?" This is one of the functions they merged. This helps remind users of products they may have forgotten to order. It also displays real-time petrol prices, enabling users to ascertain the prevailing price at their nearest ASDA petrol station. "App downloads increased by over 2 million thanks to ASDA's efforts. Even more impressive, the app's originality was recognised by IGD Digital. Mobile shopping now accounts for 18% of all household grocery purchases; of that percentage, the app generates more than 90% of the revenue. Consumers shopped 1.8% more often using mobile devices than desktop computers" (Talking Retail, 2013).

5 Understanding the term privacy

Although the right to personal privacy is almost as old as humanity, it has not always been protected by law. Also, given the huge gap between private and legally protected, why is this the case? While policies and laws are designed to protect the privacy and data security, the risks are now greater than ever. With new technologies such as smartphones, social media, the IoT, drones, biometrics, and the internet being rolled out so quickly, any new regulations enacted can become almost irrelevant. Therefore, violating someone's privacy has become much simpler over the past few decades, thanks to amazing advances in science and technology (Gautam and Malik, 2022).

The practice of keeping tabs on each other's activities has existed for a long time, especially in close-knit communities where neighbours keep tabs on each other. In today's world, not only are we seen by more people, but information about us is also preserved, sometimes with no restrictions on the nature of the data, why it is stored, or how long it will be stored. The ease with which this potentially life-changing data can be shared and organised is a boon. At this point, a person can spend their entire life online (including working, dating, and shopping) but be identifiable as unique based solely on the information and data they provide.

"Whenever new legislation is proposed that has some kind of bearing on people's right to personal privacy, it is imperative that technological advancements be taken into account. This is because technology plays a significant part" (Lukács, n.d.). "Recent inventions hinted at the widespread use of photography and newspapers, and the need for secrecy, freedom from interference, and participation in legal proceedings to defend individual rights was discussed in an article published in the Harvard Law Review in 1890. Brandeis and Warren wrote this article. This is the first time that the concept of privacy in the eyes of the law has been raised" (Dimitrios, 2022).

Cambridge Dictionary describes the concept of privacy as "the right of individuals to hide their personal affairs and relationships and to be alone and do things without others seeing or hearing you" (Cambridge Dictionary, 2022). We can see that privacy is an item with no clearly defined rights, but it does attempt to prevent or even wish to disclose personal information, such as thoughts and emotions, and how, when, and for how long. Others may transfer this personal information.

"All this data used to be difficult to collect, store and exchange, but with the widespread use of smartphones and companion apps, it has become much simpler. At the same time, protecting all your data from prying eyes is next to impossible" (Furini et al., 2020).

6 Protection and privacy of data under mobile application

It has been argued that the right to data protection exists only to support various rights and does not embody any value or interest, as its main function is to ensure the effective exercise of other rights, including privacy. Its procedural nature is validated, although it may not reflect any value. The development of computing technology and its many functions in our society has created new and urgent requirements for trust and communication between the entities authorised to process data and the individuals whose information is exploited and must be protected. By elevating data protection to the status of a fundamental right, it is easier to distinguish it from the right to privacy. At the same time, this helps to create a tool that can adapt to the changing needs of society and can provide the necessary protection (Hallinan et al., 2020). Mobile applications pose a significant threat to the privacy and data security of users for several reasons, the main ones being:

a they are software that can only be used on private mobile user devices (handheld devices)

b developing and distributing mobile applications the environmental characteristics of the program.

6.1 Safeguarding information

Most (82.7%) mobile apps use insecure encryption, while many others store data in plain text (Chatzikonstantinou et al., 2015). When a mobile device is lost or stolen, whoever finds it can access all personal and sensitive information stored on it. Encouraging users to install malware-infected mobile applications is another method of obtaining data from mobile devices (Wikipedia, 2017a).

6.2 Protecting and defending the transmissions

A client-server architecture allows most communication to occur within the mobile device. The application installed on the smartphone acts as a client and communicates with the respective databases in order to save various forms of data belonging to the user. Programmers are responsible for making sure their smartphone apps and networks can communicate with each other securely. Thanks to the proliferation of sniffing software, it's now easy for intruders to eavesdrop on your mobile device's communications with public Wi-Fi hotspots. Malicious actors can obtain a user's private information if the connection is not encrypted. Man-in-the-middle (MITM) and phishing attacks can occur if developers use insecure SSL for application server connections (Karaaslan, 2022).

6.3 Attacks utilising cross-site scripting

"An attack known as cross-site scripting (XSS) is one of the most malicious attacks against web-based applications. XSS attacks on mobile devices can result from unsafe code in hybrid mobile applications that many developers create using HTML and JavaScript. Attackers can exploit these flaws to disrupt the functionality of smartphone devices. Networking is one of the most popular activities that can be performed on

mobile devices, and adversaries can exploit XSS vulnerabilities present on trusted websites to send links to malicious applications" (Nagarjun and Ahamad, 2018).

6.4 Attacks conducted by Malware

"Malware (also known as unwanted software) is installed on mobile devices without the user's knowledge" (Wikipedia, 2017a). Malware can spread when software or websites are not properly protected. The software can broadcast messages to the entire contact list or unwanted numbers. "In addition, it can collect sensitive information and transmit it to the attacker, and if the attacker uses this malicious payload, the attacker can gain full control over the smartphone" (Mercaldo et al., 2016). Below is a list of the most common types of mobile malware.

- Worm: "Like any computer worm, Mobile Worm can replicate and spread to other mobile devices. Without the user's intervention, mobile worms can spread through text messages and other contact forms" (Tiwari and Tiwari, 2016).
- Trojan: "Such dangerous programs known as Trojan horses are embedded into trusted applications, and as soon as the user executes any of these files, the Trojan horse gets activated. Trojan horses can steal information, disable certain functions of mobile devices, and open the door for attackers to install more forms of malware" (Abura'ed et al., 2014).
- Spyware: Spyware is software that secretly gathers sensitive or personal information about a user and then sends it to third parties without the user's knowledge. This is its primary function (Wikipedia, 2017c).
- Ghost push: "Malware infects mobile devices, gains root access, installs unwanted software, repackages it as a system program, and removes itself. In order to eradicate these viruses, users may sometimes need to perform a factory reset on their mobile devices. Information about users can be stolen by such viruses" (Yang and Pan, 2015).

6.5 Utilisation of software from a third party

Most mobile apps are created by incorporating various features originally developed by other businesses rather than app developers. Developers can leverage these external libraries to monitor user activity (analytics), integrate with social media, and monetise through advertising. In addition to providing services requested by customers, the University may collect customer information. When library operators combine materials from multiple mobile applications, they can use a wealth of information to create in-depth digital profiles of their patrons (Onay and Öztaş, 2018). For example, a user can authorise one app to collect information about his or her location while authorising another app to access information about customer relationships. If two applications use the same library, the creator of the third-party library can link the two pieces of information (Achara et al., 2016). Consequently, mobile application developers rarely comprehensively understand the data collected by these services (Rodriguez et al., 2016). While doing so does not pose a security concern, it provides fertile ground for attacks if many data sources are combined.

7 GDPR

On May 25, 2018, a new data protection law, the GDPR, was implemented across the European Union (EU). In order to establish a uniform framework for processing personal data across all EU member states, the rules were developed to lay the foundations for the EU Digital Single Market. It refers to the protection, collection, and management of personal data. It applies to all companies and organisations within the EU that store or processes personal data in EU member states, as well as companies located in foreign countries that provide goods or services to people located in the EU, or track their behaviour while inside the EU (Mulder and Tudorica, 2019).

The regulations introduced by the GDPR are immediately reflected in how user data is handled. It translates the rights to know, access, and be forgotten into legal instruments in the context of active digital platforms within the EU. As a result, it empowers consumers to make decisions based on accurate information and to more easily control who has access to their data (Poritskiy et al., 2019). The requirement to provide users with more content and agency over their activities is intrinsically linked to user experience, which in turn is linked to new laws governing user interfaces (Ooijen and Vrabec, 2018).

Due to recently passed legislation, it was necessary to rethink the interface to add components to educate users about their information handling. Beyond that, their consent must be obtained, and their assets agreed to be used (Hallinan, 2020). Another modification that will impact the interface is limiting the information collected about users to what is absolutely required for each function (Crutzen et al., 2019). These changes affect the design of those interfaces, i.e., how graphical elements are used and (re)organised to maintain or improve the quality of the user experience.

7.1 Effect of GDPR on mobile applications

The ePrivacy regulations will cover services such as WhatsApp, Facebook Messenger, and Viber. These applications allow users to transmit messages or video calls over the internet. So far, laws on privacy only apply to traditional telecom companies. However, as of now, any electronic communications, such as those described above, will be considered confidential, and this will include internet-based telecommunications services. In addition, it will ensure the confidentiality of the content of the communication and the metadata associated with it, such as the location and duration of the call. This information will only be deleted or anonymised with the consumer's consent (Carmona et al., 2020).

"ePrivacy regulations ensure that the privacy of machine-to-machine interactions is never compromised". Smartphones rely on wireless communications like Wi-Fi and Bluetooth, which will disrupt them. It is necessary for a device to constantly advertise its MAC address to establish a connection over Wi-Fi. However, this information can be leveraged to discover the user's location. Given the extreme sensitivity of location information, the mechanisms by which devices communicate with each other may need to be modified (De Hert et al., 2020).

The consent process will be redesigned to be more user-friendly, and users can opt out of having their data collected. Cookies will only be used for basic functionality. In addition, users will be required to provide information about the data usage of each cookie before providing consent. All of the above affect how apps display advertisements

and how they are downloaded and used. Beyond that, it will likely impact the permissioned security paradigm used by mobile work systems.

8 Conclusions

There is an enormous growth of mobile Applications in today's world. Our day-to-day life is linked to these applications. Data privacy and security face many significant issues regarding mobile apps, especially due to the complexity of the current ecosystem of app development and development processes. Even when app developers are aware of basic regulatory obligations (from GDPR and ePrivacy law), they often have difficulty embedding these standards into their services and satisfying many constraints. This is partly due to the constraints of other parties in the environment. The benefit of mobile applications is enormous and brings benefits, not at a theoretical level but at the societal or managerial levels. New and new inventions like AI are adding benefits at a rapid pace. The biggest issue is data protection and privacy. The app provider worked a lot on data protection, but the same efforts are missing regarding privacy issues. Liberty and privacy are the two fundamental rights recognised by humankind long back, but in the present world, such violations in the name of technology are unacceptable. Yet the regulators are soft-peddling this issue. This is a clear-cut case of miss using the power of data, and researcher fears that it can lead to data terrorism. At the same time, the researcher agrees that mobile applications need softer regulatory handling to promote more innovations due to the coverage benefits, employment opportunities, and national income growth; a more constructive regulatory framework must be designed by the regulators – An e framework for E-issues. Further, businesses and nations must take collective actions like self-retainment or softer laws/pledges to fight against data misuse. Their survival is also at stake if things like data terrorism happen.

References

Abura'ed, N., Otrok, H., Mizouni, R. and Bentahar, J. (2014) 'Mobile phishing attack for android platform', *International Conference on Innovations in Information Technology*, DOI: 10.1109/INNOVATIONS.2014.6987555.

Achara, J.P., Roca, V., Castelluccia, C. and Francillon, A. (2016) *MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs*, HAL-Inria [online] https://hal.inria.fr/hal-01322286/document.

AppVerticals (2020) *Evolution of Mobile Applications: 1993-2020*, 30 April, AppVerticals [online] https://www.appverticals.com/blog/evolution-of-mobile-apps/ (accessed 20 October 2022).

Balapour, A., Reychav, I., Sabherwal, R. and Azuri, J. (2019) 'Mobile technology identity and self-efficacy: implications for the adoption of clinically supported mobile health apps', *International Journal of Information Management*, Vol. 49, pp.58–68, https://doi.org/10.1016/j.ijinfomgt.2019.03.005.

Cambridge Dictionary (2022) *PRIVACY | English Meaning – Cambridge Dictionary*, 30 November, Cambridge Dictionary [online] https://dictionary.cambridge.org/dictionary/English/privacy (accessed 5 November 2022).

Carey, R. (2022) 'Mobile app', *Wikipedia*, 25 November [online] https://en.wikipedia.org/wiki/Mobile_app (accessed 25 October 2022).

Carmona, J., Natalya, and Fernandez, F.H. (2020) 'Social media sentiment, tariffs, and international equity pricing', *International Journal of Electronic Finance*, Vol. 10, Nos. 1/2, pp.98–100.

Ceci, L. (2022) *Number of Monthly Android App Releases Worldwide 2022*, 11 November, Statista [online] https://www.statista.com/statistics/1020956/android-app-releases-worldwide/ (accessed 23 October 2022).

Chatzikonstantinou, A., Ntantogian, C. and Karopoulos, G. (2015) *Evaluation of Cryptography Usage in Android Applications*, 3–5 December, EUDL [online] https://eudl.eu/pdf/10.4108/eai.3-12-2015.2262471 (accessed 23 October 2022).

Coustan, D., Strickland, J. and Perritano, J. (n.d.) *How Smartphones Work | HowStuffWorks*, Electronics | HowStuffWorks [online] https://electronics.howstuffworks.com/smartphone.htm (accessed 23 October 2022).

Crutzen, R., Peters, G-J.Y. and Mondschein, C. (2019) 'Why and how we should care about the General Data Protection Regulation', *Psychology & Health*, 21 May, pp.1347–1357, https://doi.org/10.1080/08870446.2019.1606222.

De Hert, P., Leenes, R., Hallinan, D. and Gutwirth, S. (Eds.) (2020) *Data Protection and Privacy, Volume 12: Data Protection and Democracy*, Bloomsbury Publishing, Netherlands.

Deshwal, P. (2016) *Impact of Mobile Marketing Applications in the Current Indian Scenario*, January, GreenField Advanced Research Publishing House [online] https://garph.co.uk/IJARIE/Jan2016/3.pdf (accessed 15 November 2022).

Dimitrios, T. (2022) *Privacy and Data Protection in Mobile Applications*, 28 January, IHU Repository [online] https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/29969/Data%20Protection%20And%20Privacy%20in%20Mobile%20Applications.pdf?sequence=2 (accessed 15 November 2022).

Furini, M., Mirri, S., Montangero, M. and Prandi, C. (2020) 'Privacy perception when using smartphone applications', *Mobile Networks and Applications*, 21 February, Vol. 25, pp.1055–1061, https://doi.org/10.1007/s11036-020-01529-z.

Gautam, S. and Malik, P. (2022) 'Importance of perceived security, perceived privacy and website design of active online investors: an Indian market perspective', *International Journal of Electronic Finance* [online] http://www.inderscience.com/storage/f114716935102812.pdf (accessed 1 November 2022).

Gillis, A.S. (n.d.) *What is IoT (Internet of Things) and How Does it Work? – Definition from TechTarget.com*, TechTarget [online] https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (accessed 1 November 2022).

Hallinan, D. (2020) 'Broad consent under the GDPR: an optimistic perspective on a bright future', *Life Sciences, Society and Policy*, 6 January, p.16, https://doi.org/10.1186/s40504-019-0096-3.

Hallinan, D., Leenes, R., Gutwirth, S. and Hert, P.D. (2020) *Data Protection and Privacy – Data Protection and Democracy*, Bloomsbury Collections [online] https://www.bloomsburycollections.com/book/data-protection-and-privacy-data-protection-and-democracy/ch7-in-search-of-data-protection-s-holy-grail (accessed 10 November 2022).

Hopwood, S. (2017) *How Many Mobile Apps are Actually Used?*, 22 June, Apptentive [online] https://www.apptentive.com/blog/how-many-mobile-apps-are-actually-used/ (accessed 30 October 2022).

Insights Success (2021) *App Development Industry in India & its Dynamics*, 11 May, Insights Success [online] https://www.insightssuccess.in/app-development-industry-india-dynamics/ (accessed 30 October 2022).

Karaaslan, K.Ç. (2022) 'Analysis of the factors affecting credit card use and online shopping attitudes of households in Turkey with the bivariate probit model', *International Journal of Electronic Finance* [online] https://www.inderscience.com/offer.php?id=124478 (accessed 30 October 2022).

Keeton, N. and Wei, J. (2021) 'Development of a framework for GPS-based mobile shopping system', *International Journal of Electronic Finance*, Vol. 10, No. 4, pp.270–284.

Lukács, A. (n.d.) *What Is Privacy? The History and Definition of Privacy* [online] https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf.

Mandel, M. and Long, E. (2019) *The App Economy in India*, September, Progressive Policy Institute, Washington, DC.

Menon, N.G. (2019) *What Are the Various Phases of Mobile AppDevelopment?*, 26 September, Ognitiveclouds, Bangalore.

Mercaldo, F., Visaggio, C.A., Canfora, G. and Cimitile, A. (2016) 'Mobile malware detection in the real world', *ICSE'16: Proceedings of the 38th International Conference on Software Engineering Companion*, May, pp.744–746, https://doi.org/10.1145/2889160.2892656.

Mulder, T. and Tudorica, M. (2019) 'Privacy policies, cross-border health data and the GDPR', *Information & Communications Technology Law*, 9 July, https://doi.org/10.1080/13600834.2019.1644068.

Nagarjun, P. and Ahamad, S.S. (2018) *Review of Mobile Security Problems and Defensive Methods*, Research India Publications [online] https://www.ripublication.com/ijaer18/ijaerv13n12_20.pdf (accessed 10 November 2022).

Onay, C. an Öztaş, Y.E. (2018) 'Why banks adopt mobile banking? The case of Turkey', *International Journal of Electronic Finance*, Vol. 9, No. 2, p.95, https://doi.org/10.1504/ijef.2018.092194.

Ooijen, I.V. and Vrabec, H.U. (2018) 'Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective', *Journal of Consumer Policy*, 11 December, Vol. 42, pp.91–107, https://doi.org/10.1007/s10603-018-9399-7.

Patrick, R. (2021) 'How 5G is transforming the world of mobile app development', *Business of Apps*, 4 March [online] https://www.businessofapps.com/insights/how-5g-is-transforming-the-world-of-mobile-app-development/ (accessed 23 October 2022).

Perez, S. (2017) 'Majority of US consumers still download zero apps per month, says comScore', 25 August, TechCrunch [online] https://techcrunch.com/2017/08/25/majority-of-u-s-consumers-still-download-zero-apps-per-month-says-comscore/ (accessed 20 October 2022).

Poritskiy, N., Oliveira, F. and Almeida, F. (2019) 'The benefits and challenges of general data protection regulation for the information technology sector', *Digital Policy, Regulation, and Governance*, 23 September, Vol. 21, No. 5, pp.510–524, https://doi.org/10.1108/DPRG-05-2019-0039.

Rakestraw, T.L., Eunni, R.V. and Kasuganti, R.R. (n.d.) *The Mobile Apps Industry: A Case Study*, aabri [online] https://www.aabri.com/manuscripts/131583.pdf (accessed 23 October 2022).

Reychav, I., Beeri, R., Balapour, A., Raban, D.R., Sabherwal, R. and Azuri, J. (2019) 'How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy', *Computers in Human Behavior*, February, Vol. 91, pp.52–61, https://doi.org/10.1016/j.chb.2018.09.024.

Rodriguez, N.V., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C. and Gill, P. (2016) *Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem*, 22 September, arXiv. https://arxiv.org/abs/1609.07190.

Sharma, G. (2021) *21 Epic Mobile App Marketing Case Studies*, 4 August, Attrock [online] https://attrock.com/case-study/mobile-app-marketing/ (accessed 30 October 2022).

Subramaniam, P. (2022) *Top India App Developers*, 9 December, Business of Apps [online] https://www.businessofapps.com/app-developers/india/ (accessed 30 October 2022).

Talking Retail (2013) *Asda wins IGD Digital Innovation Award for smartphone app*, 10 October, Talking Retail [online] https://www.talkingretail.com/news/industry-news/asda-wins-igd-digital-innovation-award-for-smartphone-app-10-10-2013/.

Tikku, S.R. and Singh, A.K. (2022) 'Role of mobile banking in financial inclusion: evidence from agri traders of India', *International Journal of Electronic Finance*, Vol. 12, No. 1, pp.36–54.

Tiwari, S. and Tiwari, V. (2016) 'Bluetooth worm propagation in mobile networks', September, in *Micro-Electronics Engineering and (ICMETE), Telecommunication 2016 Conference IEEE*, pp.235–239.

WikiPedia (2017a) *Malware*, 6 July, Wikipedia [online] https://en.wikipedia.org/w/index.php?title=Malware&%20oldid=789247319 (accessed 10 November 2022).

Wikipedia (2017b) *Mobile Malware*, 28 March, Wikipedia [online] https://en.wikipedia.org/wiki/Mobile_malware (accessed 10 November 2022).

Wikipedia (2017c) *Spyware*, 2 July, Wikipedia [online] https://en.wikipedia.org/w/index.php?title=Spyware&%20oldid=788660061 (accessed 10 November 2022).

Wurmser, Y. (2018) 'Mobile time spent 2018', *Insider Intelligence*, 18 June [online] https://www.insiderintelligence.com/content/mobile-time-spent-2018 (accessed 23 October 2022).

Yan, H., Wang, J., Wang, Y. and Zhou, X. (2017) 'An example for Industry 4.0: design and implementation of a mobile app for industrial surveillance based on cloud', *2017 5th International Conference on Enterprise Systems (ES)*, September, DOI: 10.1109/ES.2017.61.

Yang, Y. and Pan, J. (2015) *New 'Ghost Push' Variants Sport Guard Code*, September, Malware Creator Published Over 600 Bad Android Apps, TrendLabs Security Intelligence Blog [online] http://documents.trendmicro.com/assets/Ghost-Push-Appendix.pdf (accessed 10 November 2022).

Yehoshua, D.B. (2016) 'Mobile sky: how KLM convinced clients to book flights on its mobile app', *Marketing Strategy*, 16 April [online] https://www.angoramedia.com/blog/klm-mobile-app-campaign (accessed 30 October 2022).