VOLUME 2 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

PRIVACY ISSUES THREATENING THE USE OF POPULAR MOBILE APPS

- Astitva Vatsa & Medha Rudra[1]

Abstract

Privacy is one of the most important and protected fundamental right by the Indian Constitution. Nowadays, as the use of technology has arisen, the importance of protecting the privacy of individuals has become more essential. Mobile devices which have become a part and parcel in the lives of people are a major source of privacy breach issues to the individuals. In the recent times, India witnessed a lot of major privacy breach from the global social networking applications and there are several such applications in our mobile devices which are always a threat for our privacy. This paper will elaborate in detail the major threats faced by the users of mobile devices. The authors will also discuss the provisions and remedies available in India for the protection of privacy of individuals. The paper will provide a detailed analysis of the major privacy controversies in popular mobile applications which are widely used by the people all over the globe. The authors will also highlight the implications on the users of such privacy breach by the popular mobile applications. This paper will emphasize on the actions taken by the Indian government, monitoring agencies and courts to protect the privacy of the individuals. So, this paper presents an overview of privacy breach issues which are threatening the use of popular mobile applications. Privacy should not be a myth in today's world but must be made a reality. Protection of privacy of citizens as well as non-citizens must be a duty of the concerned governments. So, strict regulations must be made to curb the breach of privacy and to make such mobile applications accountable for their negligence in protecting people's privacy.

Keywords: Privacy, Mobile Applications, Breach of Privacy, Threats, Protection

[1] Students at KIIT School of Law

Introduction

In today's technological era, the use and application of mobile has expanded to most sections of population. People's dependency over mobile has been increasing day by day. The increased use of mobiles created the demand of more features and uses. To fulfill these needs and demands, various mobile applications have been launched with varying features and modifications. Mobile apps are designed to run on devices like Android, iOS, etc. People use these apps by downloading from app store and installing them on their device. But with increased use, the issues relating to data privacy and protection have become a matter of concern. Mobile apps ask permission to access data from the user's device to which most people agree without reading the agreements and terms. Unrestricted mobile applications can fetch data from the user's device and such data can be used for malware attacks. Privacy is one of the most important right of an individual and it must be protected by the State for the welfare of people. In India, protection of right to privacy of citizens has been given utmost importance. Privacy is considered as one of the most fundamental right of an individual and its breach is punishable by Courts. Mobile apps are nowadays becoming a major cause in the breach of cyber privacy and personal privacy of individuals and users. Sharing of data of users to third party and misuse of such information is a major threat for users while using mobile applications. India has recently witnessed many controversial privacy breach issues by popular mobile applications which are being used worldwide by millions of users. In India, there are various provisions in various statutes for governing the privacy issues arising within the country. These provisions help in maintaining a control and facilitates the regulation of the use of various mobile applications.

Provisions in India for protection of Privacy of individuals

The protection of data being shared through the mobile apps is very essential to prevent the data breach of user's information. Although India does not have specific provisions regarding the privacy issues in mobile apps and other devices, but the Indian Constitution and few other statutes provide certain provisions for regulating data breach of individuals. Right to Privacy to

the individuals within India is guaranteed by the Article 21 of the Constitution.[2] In the case of Justice K S Puttaswamy (Retd.) &Anr. vs. Union of India and Ors.[3], the Supreme Court stated that Right to Privacy is to be considered as a fundamental right under Part III of the Constitution and it will be subject to certain reasonable restrictions. So, Article 21 also governs the privacy breach while using various applications on mobile devices. The Information Technology Act, 2000 is a major statute governing the data protection, misuse of personal information and deals with the regulations for electronic records and signatures. Section 72A of the Information Technology Act, 2000 states that it is punishable to disclose the information of an individual knowingly and purposely without taking the consent of such person and this could lead to a breach of contract.[4]This provision can be applied to privacy concerns raised by users of mobile applications. The user while installing an app on their mobile devices agree to the terms and conditions put forth by the application owner. The consent of the user to the agreement provided by the owner acts as an acceptance of agreement leading to formation of a contract between the user and owner. So this provision will be applicable in cases if the personal information provided by the user is knowingly and intentionally shared by the application owner to any third parties or to its subsidiary parts. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 states about the sensitive personal information or data of an individualincluding passwords, bank details, biometric information etc.[5] These rules are framed to protect the disclosure of such confidential information from the user's device to any other unauthorized party. One of the most important provisions in this regard is also given in Information Technology Act, 2000. Section 43A mentions the situation when a corporate body is in possession of personal data and such data is negligently implemented then such corporate will be held liable for any kind of wrongful gain and wrongful loss.[6]Right to privacy in India is considered as an element for life and personal liberty. Privacy is one of the basic essentials of an individual's personal life and the State has the

[2]Article 21 of the Constitution of India
[3]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
[4] Section 72A of Information Technology Act, 2000
[5] Vijay Pal Dalmia, Data Protection Laws in India – Everything You Must Know, Mondaq (Dec. 13, 2017), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know
[6] Section 43A of Information Technology Act, 2000

power to put restrictions on the exercise of such rights.[7] In case of privacy breach through use of mobile applications, certain amount of reasonable restrictions can be imposed by the State for the maintenance of public order and social security. So, Article 21 governs the right to privacy of individuals while their use of mobile applications and access of the personal information.

Major threats to users of mobile apps

Nowadays, there has been a significant rise in the security threats to the users of mobile apps. Mobile apps are a major source for unexpected data leakage. There are several applications in the app stores of mobile devices which are free to download but are prone to hackers and cybercriminals. The interface of such apps are easy to extract information and breach of data is a very common issue faced by the users of those apps.[8] These hacking programs present in the mobile use some distribution codes indigenous to the mobile operating systems like the Android and the iOS to transport the precious data over corporate networks without lifting red flags. The people who operate mobile phones must make sure that they only give the required permission to the apps to that extent only that it functions properly in the mobile system, so that the privacy issues can be avoided. In September 2019, updates in the Android and iOS system had been added. Some arrangement or some protocols had been inserted so that the users get aware of it and could receive knowledge about why apps collect users' location data. Programming of a data and the manner used for programming tells a lot about the threats of reverse engineering.[9] The quantity of metadata which is provided in the code is for debugging. It also helps the hacker to understand that how does the app function. Reverse engineering can be used for the privacy breach. It can be used to understand the working of the application, modifying the source code, exposing encryption algorithms, and many more and this can result in using such information against the users as hackers can take the advantage of such data.

People should regularly check the permissions and access granted to the applications in their mobile devices and should update such applicationsas per the recommendations of Android or

[7] Dr. Mohan Dewan, Personal Data Protection Laws in India, Lexology (May 13, 2020), https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d

[8] Top 7 Mobile Security Threats in 2020, Kaspersky, http://www.kaspersky.co.in/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

[9] KC Karnes, Mobile App Security Threats and Secure Best Practices, CleverTap (Apr. 1, 2020), https://clevertap.com/blog/mobile-app-security/

Apple stores or delete them if they are no longer required. Security teams of both of the operating systems have been erasing undisclosed number of apps quietly at a very increasing rate, but they have not disclosed the list of removed apps. Any particular reasons for the same has also not been disclosed by the operators. The possible reasons could be data breach, privacy breach, infringement of intellectual property, data leaking etc.The confusion regarding the disclosing of removed apps and banned apps can lead to larger risks to the individuals as such apps can still be downloaded and used due to unawareness.Phishing attacks are also very common in mobile devices as the devices are active throughout the day operating with many functions.Email apps are more prone to such attacks because they have auto-sync option in them through which mails get received and delivered automatically without any external network interference. Such email apps exhibit less details to make room for small-screen devices. We should avoid clicking on any unfamiliar email links. If the issue is not much important, then theaction or the response to such mails should wait unless and until the user is using the computer on a comparatively larger screen.

Privacy issues in Zoom

Zoom has blown up in acceptance as people have started using this video calling software since the pandemic has started. Zoom has been a boon for people who are into online school classes, yoga classes, and virtual nights out. Even the Government of India has been using Zoom to conduct the cabinet meetings. After taking so much attention towards protecting privacy of users, privacy advocates, security experts, lawmakers have warned that Zoom is facing huge privacy issue. They have even said by giving a warning that the default setting of the app are not secure enough. Zoom generates a 9 to 11-digit number that is used as ID for entering into a meeting through a call. It has been observed and noted by experts that these IDs are easy to gain access to and any random person can enter into such meetings and could create nuisances. Zoom now is dealing with the legal actions that claims that the company is unlawfully revealing the confidential information to the third parties. There were two lawsuits which were filed in

California and one is demanding for damages on part of the Zoom users for the alleged infringement of California's Consumer Privacy Act.[10]

The general issue of the Zoom security is zoombombing which allows the hackers to hack into meetings and show non-suitable content. When these people get removed by the meeting host, they many a times come back with a new account. These type of incidents happen easily because Zoom uses meeting IDs through which any random person can get access to such meetings and this makes it very unsafe for users and hosts.[11] Privacy policy of Zoom was revealed which had points which gives full authority to share the user data with third party marketers. When this was revealed in the public, Zoom again worked on its privacy policy removing those parts and declaring that now the user data is not being sold. It has also been discovered that Zoom is working all around OS restrictions by using similar methods which are also used by macOSmalware. Zoom had not responded to these concerns in much detail but the authorities have taken responsibility to look upon these privacy issues. Now tough decisions are to be taken by the company so that they can balance the default settings, privacy of the user, privacy policies to make it easier to use. The straightforward aim or approach of the company is video conferencing, but now that straightforward approach has become a crucial ingredient which has started becoming its downfall. It should get a firm holding on this matter to prevent the downfall. There were questions regarding the place of sending and receiving the data collected by Zoom from the public's computer. It was found that Zoom sends data to Facebook, even if the user is not logged in. Zoom even apologized for inappropriately routing traffic through China, where internet is deliberately monitored by government. Tech companies which are operating in China have solid dissociation between domestic and international online traffic. Zoom uses some code but not much secure end to end type. It seems as if Zoom thinks that their servers act as middleman connecting the users, count as such.

Privacy Issues in WhatsApp

[10]Tom Warren, Zoom faces a privacy and security backlash as it surges in popularity, The Verge (Apr. 1, 2020, 5:30PM), https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response

[11]Use Zoom at your own risk: Privacy concerns around this viral video conferencing app, HT TECH (Apr. 6, 2020, 4:27PM), https://tech.hindustantimes.com/tech/news/use-zoom-at-your-own-risk-privacy-concerns-around-this-viral-video-conferencing-app-story-SHZUIcBFegHvNIDKKT0vKK.html

WhatsApp had planned to launch its new and updated privacy policy on February 8, 2021 in India regarding the manner of sharing the data within the users. This led to a lot of criticisms and controversies against WhatsApp stating that the data collected by them through the users is being shared to unauthorized parties and are prone to misuse and breach of privacy. WhatsApp denied the claims of sharing the user information through its platform to its parent organization which is Facebook.[12]WhatsApp in its support stated that the new privacy policy is mainly for business accounts and does not focus much on individuals. Though it stated that accepting the new privacy policy would give them access to personal data but still they claimed that the end to end encryption would be present to provide privacy to the users. WhatsApp in its claims in Supreme Court assured the users that their new privacy aims towards providing more transparency about the collection and usage of user information and data.

The WhatsApp Controversy concerning the privacy related issues created a huge storm among the users and many users switched to Telegram and Signal from WhatsApp. The privacy issues concerning the new privacy policy of WhatsApp was challenged in Courts and it was proposed to get off with the policy as a whole and not to implement it within India. The Supreme Court in this case emphasized on the value of privacy of people and stated that people value their privacy and so it is the duty of the Courts to protect the privacy of individuals.[13] Even after the claims made by WhatsApp of not sharing the user information to Facebook, it can be noticed that during the installation process much of the personal details of the user are being collected by the application. The contact number and permission to access the gallery, contacts and notifications from the user's mobile phone is a mandatory permission to start using WhatsApp. The collecting of user's contact number can lead to serious exposure of other related personal details as mobile number is linked to bank account, Aadhar details, payment facilities of user etc. The breach of privacy can happen very easily in these ways as much of the information is already being collected and the claim of not sharing of information with Facebook cannot be completely denied. WhatsApp also stated in its launch of new privacy policy that not accepting the new

[12]Abrar Al-Heeti, WhatsApp delays privacy update following concerns over Facebook Data Sharing, CNET (Jan. 15, 2021, 1:41AM), https://www.cnet.com/news/whatsapp-delays-privacy-update-following-concerns-over-facebook-data-sharing/

[13]AnumehaChaturvedi, Supreme Court issues notices to Facebook, WhatsApp over new privacy policy, The Economic Times (Feb. 16, 2021, 3:26AM), https://economictimes.indiatimes.com/tech/technology/supreme-court-issues-notice-to-govt-whatsapp-on-plea-over-privacy-standards/articleshow/80920387.cms

terms and conditions will lead to unavailability of all features in the version of WhatsApp the user is using. This is a breach to the user's privacy as forcibly collecting personal information of the individual without his voluntary agreement to the privacy policy is detrimental to the interests of the user. Due to all the commotion caused after the announcement of the launch of new privacy policy and following the apex court's decision, WhatsApp has decided to delay the updating of its privacy policy from February 8, 2021 to May 15, 2021.

Privacy issues in Amazon

There have been many issues with Amazon. There are many cases which involve entities trading fraud commodities on Amazon. Though Amazon is continuously working and taking action on these issues, still there are many examples of these type of cases which slip out from Amazon's system without getting detected. Amazon has been criticized for this particular issue, but there are many more cases apart from this. People also talk about the biggest privacy issue of Amazon that is Alexa. One thing that Amazon gets advantage over its competitors is that it sells electronic devices that it manufactures together with software and services provided with the devices. Amazon has been asked on various occasions that what data type does Amazon collect through the echo devices by the lawmakers. Basically, the regulators want to gain the knowledge that the devices which are sold by them, how do these devices listen to people, and what happens to data which is sent to Amazon. It is very common or usual knowledge that Amazon is gathering details about the discussion and linkage with the Echo devices. It has also been proved that Amazon's data collection methods have bugs that places user data's privacy into compromise. People are not so amenable with the thought of being monitored from outside and people should be allowed to choose that how they are recorded.

It's very difficult to determine that what happens to the data when it enters the Amazon's servers due to unclear or vague revelation documents. Amazon processes a big amount of data that is transferred all over the internet through their software, Amazon Web Services and visitors to their websites.[14] This particular data is to feed the artificial intelligent system by the Amazon so that it's marketing decisions becomeeffective and their services get improved. Amazon devices

[14]Privacy Issues with Amazon, Choose to Encrypt (Sep. 11, 2019), https://choosetoencrypt.com/privacy/privacy-issues-with-amazon/

which include Echo and Fire Tablet also collect data for Amazon. Amazon has acquired itself to use data to enhance customer experiences. There are many of them who want to protect their data, maintain privacy with it, but there are many convenient offers that Amazon provides and no one is willing to give up these conveniences. People who are really serious about their privacy have given up Amazon altogether, but for many Amazon has become important in everyday life. To avoid tracking, it is possible that people can avoid internet connected devices, but for many people, their jobs are dependent on these tools. Even if Alexa and the other Echo devices are listening to its user's demand every time but they are not expected to record everything. If this data is being recorded, much can be revealed about someone. When data which Alexa is recording gets deleted, the ability to serve people gets reduced by Alexa which unluckily is the issue that we have got used to.

Privacy Issues in Facebook

Facebook is one of the most popular social media networking application which is being used globally by millions of users. With popularity comes the responsibility to protect the interests of the users and to build a trustworthy relationship between the company and the users. Facebook also got caught in controversy when it collected the user's data without their consent by linking one account to another. In 2014, the users of Facebook got an invite to participate in a quiz on the application which will help the users in finding out their personality type based on the answers they give to the questions asked. Facebook collected the data including personal information from the application accounts of the users who participated in the quiz. The privacy concern was raised when along with the data collection of participants, public data of friends of such participants was also collected by the application. The quiz was attempted by around 305,000 users but the data collection was done for around 87 million as reported by Facebook.[15] It was alleged that some parts of the data which was collected was sold to a company named 'Cambridge Analytica'. The breach of privacy is caused when it was claimed that Cambridge Analytica used such public information of the users to psychologically profile voters in the US Presidential Elections. Though Cambridge Analytica denied the claims, this incident shook the trust of users and created a concern for the information stored in Facebook by the users. This is a

[15] Facebook to pay record $5bn to settle privacy concerns, BBC (Jul. 24, 2019), https://www.bbc.com/news/business-49099364

breach of trust caused by the Facebook to the users as they could not provide proper security safeguards for collecting and storing public and personal information of the users of the application. The data collected through the Facebook and its access to Cambridge Analytica caused a major scandal across the globe because many other private parties took advantage of such information without any authorization from Facebook or its users. A fine of £500,000 was imposed as a penalty on Facebook by the UK privacy protection laws for not properly safeguarding the personal data of the users. Mark Zuckerberg said in his statement that "Facebook is reviewing its technical systems to identify possible privacy risks, and going forward, whenever the social network built a new product that used data, or a feature changed the way it used data, possible privacy risks would need to be addressed." The impact of Cambridge Analytica was also a matter of concern for the company. CA got bankrupt by 2018 and lawsuits were filed against it for destroying and deleting the collected information and data of the users. Facebook faced a lot of criticisms after this incident and it assured to focus more on privacy protection of users. Recently, Facebook again was alleged to access the personal information of the users of WhatsApp and it is trying to come up from the claims raised against it.

Actions taken to prevent the popular privacy controversies

The Constitution of India guarantees the right to privacy as a fundamental right. In August, 2019, Right to privacy was upheld by a nine judge constitutional bench in Supreme Court. According to the Supreme Court's decision, right to privacy has been scrutinized into two articles of Constitution: Article 21 which has Right to life and Liberty, and Part III which is a Chapter on Fundamental Rights in the Indian Constitution.[16] This totally signifies that any restriction upon the reasonable restrictions must not only convince the tests developed under the Article 21, but also where breach of privacy results to contravention on the other rights, such as disturbing outcomes of analysis on free speech, a constitutional framework at present lives for the cases to be heard inside. Till date, there have been a number of landmark cases where the Courts have acknowledged right to privacy as fundamental right. One such case was of Kharak Singh v. The State of U.P.[17] in which the judges pinpointed that right to privacy is placed under the right to

[16] State of Privacy India, Privacy International (Jan. 26, 2019), https://privacyinternational.org/state-privacy/1002/state-privacy-india

[17] Kharak Singh v. The State of U.P., 1963 AIR 1295

personal liberty in addition to freedom of movement. Judgement of Supreme Court also validates decisions which were made thereafter Kharak Singh on privacy, subject mattered to above conditions. Another one was Govind v. State of M.P.[18] in which Supreme Court substantiated that right to privacy is a fundamental right. It was said that the right to privacy was to enclose and safeguard the personal togetherness of the home, motherhood, family marriages, generation and child nurturing. Although, right to privacy is put through "compelling state interest".

India is in coalition with two universal apparatuscarrying privacy protections. They are the International Convenant on Civil and Political Rights (Article 17) and Universal Declaration on Human Rights (Article 12). Keeping in mind the Mumbai terrorist attack in the year 2008, India executed a broad range of sharing of data and observation plans so that the security and public safety gets increased by challenging crime and terrorism. But somehow these projects have since then uplifted many privacy concerns. Central Monitoring System was visualized to cluster the avoidance of communication data and sanction law enforcement agency entry to it. If it gets executed, it would get linked and connected to the Telephone Call and Interception System (TCIS) which would help observe the voice calls, fax communications on landlines, MMS and SMS, video calls, CDMA, 3G and GSM networks. For naming some more, there are a few schemes and projects which embraces NATGRID, Lawful Intercept and Monitoring (LIM) systems, and CCTNS Project. Indian Government is trying to make and bring every possible law so that the right to privacy issues do not concern and disturb the people, whether personally or for the information that is confidential about the country or the state.

Conclusion

Protection of the right to privacy as guaranteed under Part III of the Indian Constitution is an essential element for all the individuals, companies and State. With the advent of technology, the risks are increasing day by day, which necessitates the improvement of privacy protection safeguards more effective and strong. Mostly, social networking applications are prone to privacy issues and malware attacks. From the user's part of action, the terms and conditions of the mobile applications must be read twice by each user before giving an application access to

[18] Govind v. State of M.P., 1975 AIR 1378

the mobile device. Any kind of unauthorized access to non-verified apps should be prohibited. The application providers must be more concerned about protecting the users' personal information which is collected, stored and is being shared through their mobile applications. The trust between the provider and user must be maintained at all costs. The encryption pathways must be more effective and loopholes should be repaired as soon as it is found out. Privacy is one of the protected fundamental rights in India. The State should value peoples' privacy over any other mobile applications. An individuals protected privacy becomes the reason of personal liberty of such individual. Specific laws, rules, regulations and guidelines needs to be formulated in order to govern the use of mobile applications so that the breach in privacy could be avoided to a great extent. This will help in making parties accountable and liable in case any kind of breach of privacy occurs through the configuration of their mobile applications. As Gary Kovacs has rightly said' "Privacy is not an option, and it should not be the price we accept for just getting on the internet." So, even in this socially and virtually active era, an individual must have the full rights over his personal and public information and should decide what all to share and what not to be shared.