A Review and Survey on Smartphones: The Closest Enemy to Privacy

Priyanka Jayakumar, Lenice Lawrence, Ryan Lim Wai Chean, and Sarfraz Nawaz Brohi(✉)

Taylor's University, Selangor, Malaysia
{Priyankas.Jayakumar, Lenicelawrence, Ryanwaichean.Lim}@sd.taylors.edu.my, SarfrazNawaz.Brohi@taylors.edu.my

Abstract. Smartphones have changed the world from a primitive to a high-tech standpoint. However, there have been many incidents where third parties have used confidential data of the users without their consent. Thus, it causes people to be paranoid and distrustful of their smartphones, never knowing which application threatens to expose them. In this paper, we have conducted an in-depth review of the significance of smartphones in human life, and we have discussed the methods used by various authorities to collect and exploit users' data for enigmatic benefits. Moreover, we surveyed the smartphone users to identify the vulnerabilities leading to privacy violation, and to examine their knowledge about the protection mechanisms. We determined that Technology and Human are the two major vulnerabilities that are exploited to invade users' privacy. It is the necessity of the moment for the researchers and developers to formulate solutions that could be used to educate and protect smartphone users from potential threats and exploitation of data.

Keywords: Smartphones · Privacy · Data exploitation · Mobile applications

1 Introduction

Smartphones have revolutionized human life due to features such as connectivity, efficiency, functionality, and entertainment [1–3]. Connectivity: Besides phone calls and text messages, one can access social networking sites like Facebook, Twitter, SnapChat and many more. Advanced connection services like Viber and Skype enable one to save money through free conversation. One can also send and receive emails once their email accounts are set up and synced to their phone. Efficiency: Smartphones are efficient because they speed up processes making it easier for people to go about their business on the move. Applications such as Google Docs and OneDrive allows a person to work and collaborate with other people anywhere and anytime without the aid of computers. Functionality: Other than connectivity and efficiency, there are abundant applications for various purposes that can be installed on a smartphone. Smartphones provide users, the choice of enabling security measures to protect important data on their devices. Entertainment: One of the main attractions of smartphones is the entertainment factor. Latest movies, songs, TV shows and even online

M. H. Miraz et al. (Eds.): iCETiC 2019, LNICST 285, pp. 106–118, 2019.
https://doi.org/10.1007/978-3-030-23943-5_8

gaming has been accessible on the move using smartphones. The discussion of smartphones being an invasion of data privacy never ends. Smartphones are great pocket-assistant devices because they contain a variety of sensors [4]. Since smartphones have become a necessity, people rarely go without them. This enables the sensors to gather users' data. These sensors are both a gift and a curse. This is because the sensors could be compromised for malicious intents without users' knowledge. For example, online app store Google Play removed 20 apps because they were abusing their access through sensors found on Android phones. This means before Google discovered the privacy violation conducted by these apps, they could track and keep a record of users' most private data like their current location, pictures, videos, sensitive files and everything else on their devices. Besides providing opportunities for hackers or perpetrators to snoop into users activities via sensors, certain apps on smartphones gather data such as recently searched, most popular search, and download history. The developers have built the apps in such a way that they compile all the raw data and then sell them off to advertising companies, which then convert them into useful information and ultimately, profit. It may seem harmless on the surface, but there may be data that the user would have wanted to keep private and confidential. For example, randomly searching for a product on a search engine could cause pop-ups or e-mails regarding the same searched product at a discounted price. In order to contribute to the domain of smartphones data security, we conducted this research to identify the user and technology related vulnerabilities. The findings from this research could be used as strong foundations to carry out advanced research in the domain especially related to protecting smartphone users from data privacy violation and to make smartphones a trustable next-generation technology. The rest of this paper is structured as follows: In Sect. 2, we discuss the secret methods of data collection using smartphones. Section 3 contains a discussion on the exploitation of the data. The survey results are analyzed in Sect. 4 and critically discussed in Sect. 5. Finally, we have concluded the research in Sect. 6.

2 The Data Collection Methods

Unauthorized data collection is a major concern among the general population in today's age. Due to the vast upgrades and constant improvements in technology, devices are being more necessary than ever in a society. Smartphone devices have become almost like a necessity in today's world, and base models are getting increasingly more affordable [7]. What would have cost thousands of dollars previously, could be only a couple of dollars today. This is one of the many reasons that the use of smartphones is widespread with some users being as young as three years of age. Users of devices like smartphones should be constantly aware of the permission that they grant the phone, if they are not, their data can be collected even without them realizing it. There are many ways through which smartphone users' data can be accessed. The data collection methods are discussed in the following sub-sections.

2.1 Location Sensors

Location sensors determine the exact geographical location of smartphone users with high accuracy. Longitude and latitude coordinates obtain the geographical location, but its accuracy is dependent on the types of applications, operating system and hardware of the smartphone [8]. As more users are using phones for navigational purposes as well as transport services, the majority of smartphones being produced have high accuracy location sensors embedded in them. Some of these location sensors measure not only the latitude and longitude but also an 'x' element, which refers to the height or elevation of the device. This allows for more accurate tracking and data collection. The applications of an iOS and Android device are different. Apple is stricter when it comes to granting location permission to an application, and allows the user to adjust these settings, both via the application, as well as through the device privacy settings [9]. For Apple, users can select between having the location of the device always turned-on, always turned-off or be turned-on only when an application with permission is open and running. However, for Android, users may need to take extra precautions. In an investigation and report by Quartz, it was found that even if the smartphone device is actively turned-off, the device is without a SIM card, is not connected to the internet, and does not have any applications needing location services to be used, Android OS phones can still collect location data to be sent to Google as soon as the smartphone is connected to the internet. When the application has location access or if the device itself has location access turned-on all the time, data is being collected constantly. Certain smartphone applications can even figure out roughly what floor of a high-rise building that you work or stay in based on time and frequency of visits [10].

2.2 Accelerometer and Gyroscope

Most older smartphones have had accelerometers that measure in only one dimension. However, the latest smartphones have accelerometers that measure in three dimensions, with these dimensions being 'x', 'y' and 'z'. This is also known as the three-axis accelerometer. Apart from this, a gyroscope is also available on most devices [11]. This allows not only the speed to be measured but also the relative positioning and direction of travel of the smartphone device. A certain travel company who has monitored these data has found that in their application, the number of visitor's peak and surge around midnight, which is right before most adults head to bed. It was also found that during these times, the devices (mainly smartphones) that are being used had many rotations going on. This indicated that a majority of the users were looking at travel sites while lying in bed, as lying on their side generally causes the phone to rotate to landscape mode.

2.3 Wi-Fi Sensors

Another way of gathering data is through Wi-Fi. The monitoring and data gathering of location-based data via Wi-Fi is one of the lesser-explored uses of Wi-Fi. However, it is a good way to get these location-based data as it uses less battery as compared to GPS or accelerometers [11]. With Wi-Fi sensors, the location of a user can be extracted

based on which access points they have connected their device to. Other data that can be gathered from Wi-Fi access points are the speed or if the user is currently traveling. This data is gathered by measuring the speed of the connection changes as it may rapidly connect and drop, thus assuming if the user of the smartphone device is traveling at a relatively high speed. Even if the smartphone device does not connect to a Wi-Fi network, it can still be traced, and data can be collected based on the fact that smartphone devices usually automatically scan for Wi-Fi connections through various access points [12]. These access points can be tracked as smartphone devices can measure various components such as the access point's MAC address, its SSID's, name and signal strengths.

2.4 Virtual Keyboards

A Virtual Keyboard (VK) is a vital part of any smartphone, as the majority of the things we do on a smartphone needs a VK to function. Another reason it is important is that every piece of information from mundane daily memos to private credit card numbers and other passwords go through the VKs [3]. Some VKs require a login account to personalize data such as words and phrases that are commonly used. However, it is highly likely that these VKs sell the data to third-party applications or companies for targeted advertising [13].

2.5 Third Party Tracking Applications

A study has shown that about 70% of applications share the data collected with companies such as Google analytics [14]. Companies like these can obtain data from various applications and combine them to form a scarily accurate and detailed profile of smartphone users [15]. They can combine information to do this even if all applications are granted permissions separately [12]. However, big companies like these have one goal in mind, i.e., profit. The main source of this profit is to create and deliver specific and targeted advertisements based on what the tracking applications have identified to be interesting to the smartphone user.

3 The Exploitation of Data

There are many different purposes for organizations or authorities to obtain users' data. However, most of these reasons lead back to one cause, i.e., profit. [16]. When we say that data is unethically, illegally or inappropriately used, it means that the original owner of the data did not consent to the data being used in that specific manner. This section contains information about the uses of data that are unethical, illegal, or a combination of both.

3.1 Targeted Advertisements

Targeted advertisements are dedicated to specific products or services that interest a user. This is achieved by collecting various user data using many applications,

especially social media based apps. Some of the most used categories of data for targeted advertisements are; location, search history, browsing history, posts viewed or interacted with on social media, pictures seen or videos watched, and even certain key terms based on keyboard activities. Location-based advertisements gather location data from GPS of the device to deduce the locations that the user is most often at, as well as locations that have been visited or areas checked in on various social media apps [17]. The advertisements presented may be related to travels, services or goods provided near those locations. For search history and browsing history, the advertisements would be items or services that have previously been searched or looked for. Data from posts viewed or interacted with, pictures looked at or videos watched, will generate data that will produce advertisements of similar topics or items related to recently viewed activities. Finally, it would be keyboard activity, which is the most privacy invading option. The data stored could be anything from credit card information to passwords to words that are often used. This information will be used to find advertisements that are related to these words.

3.2 Selling Data

Numerous third-party firms would buy the data to be analyzed. Companies can also use this data for themselves. For example, The Wall Street Journal has cited two cases relating to this; A travel website charging Mac users' higher hotel prices, and a large multinational office supply chain offering better deals only if there is a competitor within a 20-mile radius. The travel website, Orbitz, found out that Mac users were more likely to spend up to 30% more on a hotel room, and they were 40% more likely to spend on 4 or 5 star hotel rooms as compared to Windows users [18]. Thus, they have started providing Mac users with higher hotel room prices to increase their profits. As for the office supply store Staples, the Wall Street Journal has found out that Staples is tracking the location of online users and only offering discounts and coupons if there is a competitor store within a 20-mile radius from their current location [19]. If no competitors are found nearby, Staples assumes that the users are willing to pay the higher price as they do not have a choice, thus eliminating the discounts and coupons for these users and increasing their profits.

3.3 Candidate and Employees Profiling

New companies tend to do screenings on potential employees or the employees that they feel they may need to worry about. Companies and organizations these days will either look up the employee on social media and various search engines or get investigators to find out more about these employees. Not all companies or organizations will have the resources to hire investigators, nor need to if it is not a high position. Facebook has been found to publicly display users' data even if the user has restricted it to the 'friends only' option [8]. This enables employers to check Facebook pages of potential or current employees. This is unethical on the part of Facebook, as users have restricted these data or contents to specifically their friends only, and not the general public.

3.4 Predicting and Influencing Users Habits

Similar to the targeted advertisement, the data collected is used by marketers to try to influence certain users to purchase certain products or services. The difference from targeted advertisements is that the user may not have shown interest in these products before, and these advertisements are usually decided based on demographics or personal data. The data collected will be used to promoting certain items, which they feel the user may be inclined to buy. A well-known example of this was certain cigarette companies targeting their advertisements towards highly stressed and lower-income users, as it was this group of people that were most likely to start smoking and buy cigarettes [20]. A user dependent on cigarettes is a loyal customer to them, thus increasing their profits constantly.

3.5 Distribution of Confidential Data

There have been multiple cases where personal data had been stolen and published on the internet for everyone to see. A few common cases were the nudes of celebrities stolen via iCloud and published, and when accounts of dating site users were published. In the first case, which happened in 2014, a hacker gained access to the iCloud library of Apple used by celebrities and leaked their personal and private photos online [21]. The hacker gained access to the iCloud accounts via brute force attacks and followed up by publishing a list of 100 celebrity names whose accounts had been supposedly hacked, followed by uploads of photos soon after. In the second mentioned case, occurred in 2015 when a hacking group accessed and stole users' data of a site called Ashley Madison. The Ashley Madison site was a dating site targeted towards individuals who were married or in a relationship. These hackers believed that what they did was ethical as they were exposing cheating and unfaithful individuals. However, the fact that they had hacked into, and stole 60 GB worth of user profiles and data, along with identifying and real-world profiles, is illegal [22]. This data leak has caused many problems towards the affected individuals, ranging from the breakdowns of families, discrimination among their peers, and was even linked to two cases of suicide. Regardless of whether the hackers believe that their stealing of data is for ethical reason, the act in itself is illegal and wrong. The users entrusted the companies with keeping their profiles and data secure and did not consent to their data being openly uploaded online for others to view. It is a serious breach of personal and private data and can have many negative effects on the victims.

4 Survey

This section analyses the survey conducted to identify the user vulnerabilities that could lead to privacy violation using smartphones. Additionally, we aimed to understand how users feel about their privacy concerning smartphones. This survey has 202 responses from participants of different age groups, geographical locations, and opinions on smartphones data privacy. We started with a question to determine the data that participants find the most private to them. 151 participants (74.8%) consider

passwords on their devices to be the most confidential data. Coming close to that number, 103 participants (51%) declared photos and videos are most private to them. 90 participants (44.6%) find emails, and a total of 80 participants (39.6%) stated that location is the most sensitive data to them, respectively. The remaining participants have considered documents, banking details, messages, chat history, and contacts as the most private data as shown in Fig. 1.

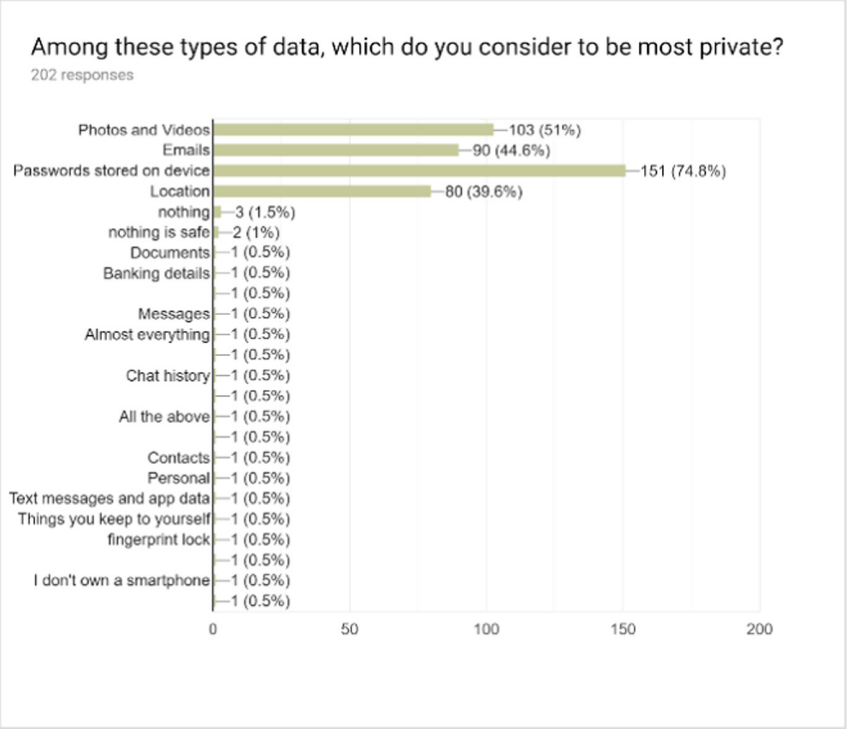

Fig. 1. Data importance.

In the world of smartphones, the application level permissions could potentially lure users into collecting their sensitive information. The second and third question was targeted to understand the users' interaction with the permissions required by the apps. As shown in Fig. 2, 49% participants occasionally, 26.7% participants have never, and 24.3% participants make it a point to read all the required permissions before installing or using an application on their smartphones. This finding is bothersome because only a minority of the participants read all the permissions requested by an application before installing it. This is probably because the permissions are too lengthy to read or the need for the application is greater than data privacy or simply due to lack of knowledge. Moreover as shown in Fig. 3, 62.9% of our participants had refused to install an application when it asked for certain unrelated permissions. Of the remaining

participants, 23.8% have never, and 13.4% have refused to install an application once due to the permission it requested, respectively.

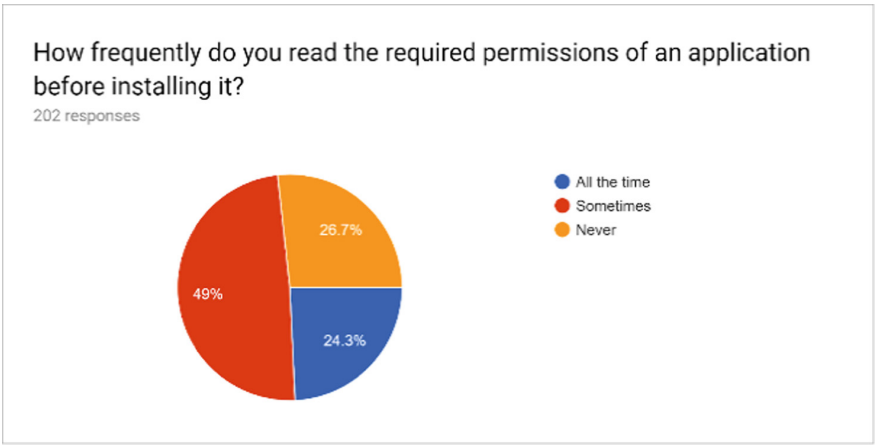

Fig. 2. Users knowledge.

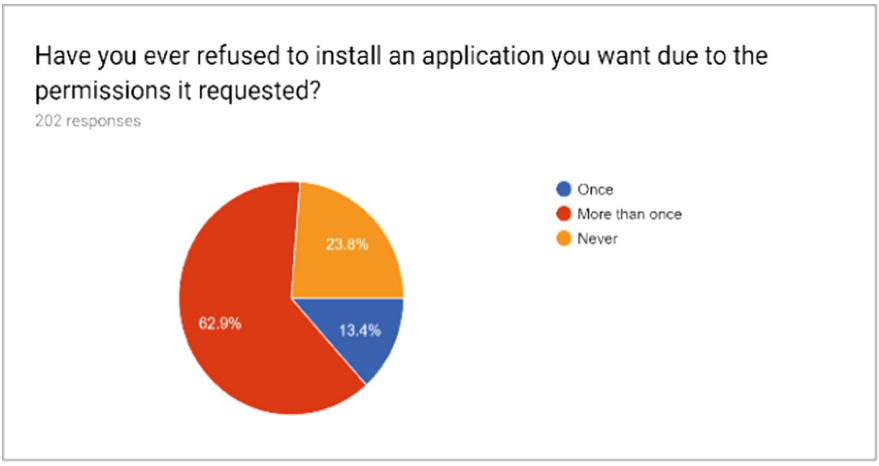

Fig. 3. Application permissions.

The fourth and fifth question was targeted to identify the protection mechanisms and precautionary measures undertaken by the users as a defense mechanism against the privacy-violating Apps. As shown in Fig. 4, we are amazed to determine that 42.6% of participants have never used anti-virus and anti-malware applications on their smartphones, 31.7% are currently using either anti-virus or anti-malware on their devices, whereas 25.7% used to have one of those two types of applications but not anymore since they uninstalled it. Moreover, as shown in Fig. 5, 60.4% participants

have not installed applications outside of Google Play Store or Apple App Store, while 38.6% has confessed to having installed applications outside of the certified application installation platforms and trusted sources. This number is worrisome because participants open doors for many malicious applications that can invade their privacy.

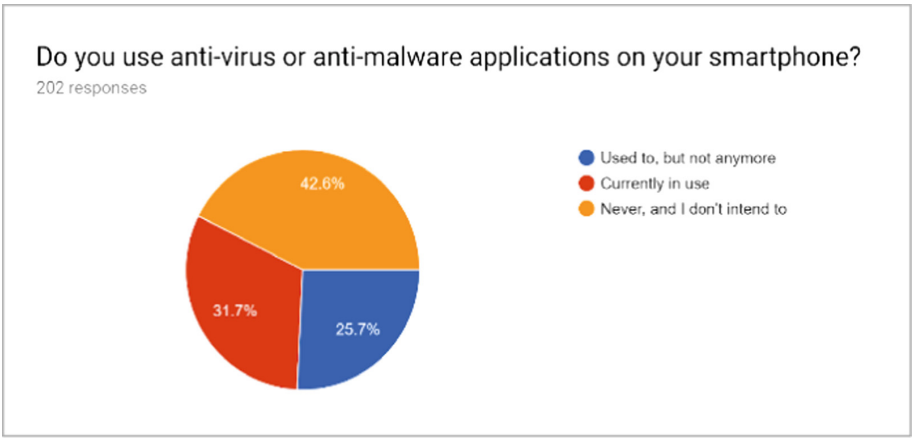

Fig. 4. Using protection application.

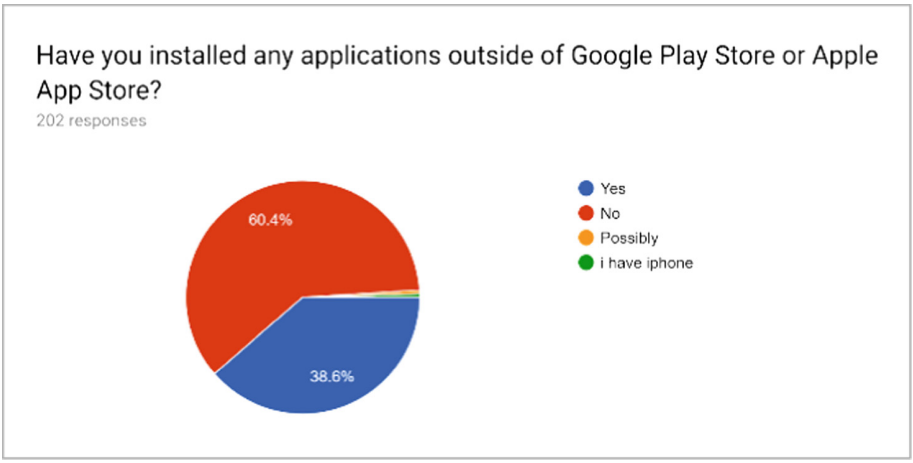

Fig. 5. Trusted and untrusted applications

5 Discussion

From the overall survey results, we observe that smartphone privacy issues occur due to two major vulnerabilities (Human and Technology). The smartphone technology has been developed to enable communication, collaboration and to assist users in a variety

of other everyday tasks. However, likewise any other technology, this technology can and has been exploited for malicious reasons. The intruders such as hackers and organizations are spying on user activities, collecting data for personal gains such as advertisement, service improvement, and selling data. The smartphone users are vulnerable to various threats, and in most cases, they are unaware of the effects on their data privacy. However, in certain cases, users indirectly or unintentionally allow access to their sensitive data due to lack of awareness and knowledge of the smartphone technology and the apps. Many of the users are not even aware and well informed of using protection mechanisms such as anti-virus, anti-malware, and other anti-spyware services. Furthermore, the users of smartphones are also not conscious of the permissions that apps require from them during the installation or execution time. In certain cases, the users grant unwanted permissions to the Apps due to their need and convenience to use the required features. The lack of care in granting permissions could lead to privilege escalation, and users' data privacy can be at risk. It is the necessity of the moment for the researchers and developers to formulate solutions that could be used to educate and protect smartphone users from potential threats and exploitation of data.

There are solutions developed to deal with issues regarding the required permissions of a mobile application. When people download an application, they do not read the app's privacy policy because it is tedious and filled with complicated words that they may not understand [23]. To address this issue, the mobile application market should be plastered with application reviews that come from trusted sources. This will give users a sense of relief knowing that their data will be secured from third-party exploitation. Brands also serve their purpose by building a reputation of being responsible for maintaining the privacy of user data so that users will not have any qualms from downloading any mobile application developed by them. A balance needs to be struck between users of apps who want their data to be secured and the app developers who want to boost their revenue by using user profiles for advertisement purposes [24]. To do this, a new model must be developed that will have two distinct flows of information, one from the user to the developer and another from the user to the advertisement network, both vice versa. Both developers and ad-networks will have unique privacy requirements. The application developer has certain privacy requirements that work in conjunction with the application while the ad-network can develop privacy methods that will fully aid the market reliant on advertisements. A solution to privacy risks in the form of an anonymous identifier has been presented [25]. Blockchain can also be used to protect data that users want to keep private [26]. The blockchain system involves two main proceedings, the protection of users' data and the ability for services to retrieve the data after a verification process using digital signatures. To better ensure that users are aware of the available mobile applications that consist of effective privacy and security features, an app recommendation system is a solution [27]. TaintDroid is a system designed to keep track of the usage of private data by third-party applications that may or may not be suspicious on Android [32]. Data from both reputable and non-reputable apps will be tainted. Whenever it is found that the data has been shifted from 1 location to another, TaintDroid will create a log of the event containing the details of the movement of the data, painting a clearer picture as to which apps are credible and which are not.

6 Conclusion

Cyber-criminals who are utilizing a highly sophisticated range of approaches and destructive codes, are aiming conventional operating platforms such as iOS and Android [33]. There is a legion of operating system versions in use to cater to the ever-increasing number of smartphone users on Earth [34]. While conducting this research, we realized that smartphone technology is a double-edged sword. It brings many benefits and makes lives very convenient but also presents several risks to user data stored within it. The privacy problems posed by smartphones are phishing attacks through location tracking, racial profiling, user surveillance and controlling the smartphone camera for spying purposes. Some solutions we have discovered include increasing the number of trusted reviews for applications, blockchain security and app recommendation systems. In our survey, we have discovered that fewer users read the terms and conditions of the application before installation. Almost half of the participants do not have antivirus or anti-malware apps on their phones, leaving them vulnerable to attacks. Finally, nearly 40% have downloaded an app from an untrusted site increases the chances of compromising their phone because these applications might be virus or worm infected.

References

1. John, J.: Why are smartphones so important in daily life? - Trffc Media (2018) Trffcmedia.com. http://www.trffcmedia.com/topics/why-are-smartphones-so-important-in-daily-life/
2. Targetstudy.com: Importance of smartphones in our life (2018). https://targetstudy.com/articles/importance-of-smartphones-in-our-life.html
3. Wang, D., Xiang, Z., Fesenmaier, D.: Smartphone use in everyday life and travel. J. Travel. Res. **55**(1), 52–63 (2014)
4. Temming, M.: Your phone is like a spy in your pocket (2018). Science News. https://www.sciencenews.org/article/smartphones-data-collection-security-privacy
5. DeMuro, J.: 8 reasons why smartphones are privacy nightmare (2018). TechRadar. https://www.techradar.com/news/8-reasons-why-smartphones-are-privacy-nightmare
6. Hoffman, S.: Your smartphone or laptop camera: a window into your private life? (2018). InCyberDefense. https://incyberdefense.com/original/smartphone-laptop-camera-private-life/
7. Weinstein, M.: 13 ways your online privacy was violated in 2016 - and what you can do about it (2018). Mirror. https://www.mirror.co.uk/tech/13-ways-your-privacy-violated-9479084
8. University, S.: Unauthorized transmission and use of personal data (2018). Scu.edu. https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/
9. Ng, V., Kent, C.: Smartphone data tracking is more than creepy – here's why you should be worried (2018). The Conversation. https://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110
10. Baraniuk, C.: Phone sensors can save lives by revealing what floor you are on (2018). New Scientist. https://www.newscientist.com/article/2152366-phone-sensors-can-save-lives-by-revealing-what-floor-you-are-on/
11. Garnett, O.: Beware the power and pitfalls of mobile data collection (2018). Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/04/18/beware-the-power-and-pitfalls-of-mobile-data-collection/#4162ef4c40dc

12. Goode, L., Ceres, P., Pardes, A., Barrett, B., Goode, L., Barrett, B.: App permissions aren't telling us nearly enough about our apps (2018). WIRED. https://www.wired.com/story/app-permissions/
13. Kromtech, S.: Virtual keyboard developer leaked 31 million of client records (2017). Kromtech.com. https://kromtech.com/blog/security-center/virtual-keyboard-developer-leaked-31-million-of-client-records
14. Narseo Vallina-Rodriguez, T.: 7 in 10 smartphone apps share your data with third-party services (2018). Scientific American. https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/
15. ICSI: The ICSI haystack panopticon (2018). Haystack.mobi. https://www.haystack.mobi/panopticon/
16. Guest, C.: On the ethical use of data vs. the Internet of Things (2018). Forbes. https://www.forbes.com/sites/ciocentral/2016/12/21/on-the-ethical-use-of-data-vs-the-internet-of-things/#3982da7e1247
17. Shermach, K.: Data mining: where legality and ethics rarely meet (2018). E-Commerce Times. https://www.ecommercetimes.com/story/52616.html?wlc=1245363355
18. Mogg, T.: Orbitz travel website directs Mac users to pricier hotel options | Digital Trends (2018). Digital Trends. https://www.digitaltrends.com/apple/orbitz-travel-website-directs-mac-users-to-pricier-hotel-options/
19. Jennifer Valentino-DeVries, J.: Websites vary prices, deals based on users' information (2012). WSJ. https://www.wsj.com/articles/SB10001424127887323777204578189391813881534
20. Connolly, G.: Tobacco companies target poorer neighborhoods with advertising (2010). News. https://www.hsph.harvard.edu/news/hsph-in-the-news/tobacco-advertising-poor-neighborhoods/
21. Cellan-Jones, R.: Apple: celebrity accounts hacked (2014). BBC News. https://www.bbc.com/news/av/technology-29032705/apple-celebrity-photos-targeted-by-hackers
22. Lord, N.: A timeline of the Ashley Madison hack (2017). Digital Guardian. https://digitalguardian.com/blog/timeline-ashley-madison-hack
23. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, p. 1. ACM, July 2012
24. Leontiadis, I., Efstratiou, C., Picone, M., Mascolo, C.: Don't kill my ads!: balancing privacy in an ad-supported mobile application market. In: Proceedings of the Twelfth Workshop on Mobile Computing Systems and Applications, p. 2. ACM, February 2012
25. Beach, A., Gartrell, M., Han, R.: Solutions to security and privacy issues in mobile social networking. In: International Conference on Computational Science and Engineering, CSE 2009, vol. 4, pp. 1036–1042. IEEE, August 2009
26. Zyskind, G., Nathan, O.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops (SPW), pp. 180–184. IEEE, May 2015
27. Zhu, H., Xiong, H., Ge, Y., Chen, E.: Mobile app recommendations with security and privacy awareness. In: Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 951–960. ACM, August 2014
28. Liang, X., Zhang, K., Shen, X., Lin, X.: Security and privacy in mobile social networks: challenges and solutions. IEEE Wirel. Commun. **21**(1), 33–41 (2014)
29. He, D., Chan, S., Guizani, M.: User privacy and data trustworthiness in mobile crowd sensing. IEEE Wirel. Commun. **22**(1), 28–34 (2015)
30. Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., Luo, H.H.: Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wirel. Commun. **22**(4), 104–112 (2015)

31. Kotz, D., Gunter, C.A., Kumar, S., Weiner, J.P.: Privacy and security in mobile health: a research agenda. Computer **49**(6), 22 (2016)
32. Enck, W., et al.: TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Trans. Comput. Syst. (TOCS) **32**(2), 5 (2014)
33. Finjan Mobile: Mobile device privacy and security challenges and recommendations (2018). https://www.finjanmobile.com/mobile-device-privacy-and-security-challenges-and-recommendations/
34. Tsavli, M., Efraimidis, P., Katos, V., Mitrou, L.: Reengineering the user: privacy concerns about personal data on smartphones. Inf. Comput. Secur. **23**(4), 394–405 (2015)
35. Kaspersky Lab, Android Mobile Security Threats. Daily English Global. https://www.kaspersky.com/resource-center/threats/mobile
36. Warner, C., Smartphone attacks: 7 reasons why hackers have shifted their target. Wandera. https://www.wandera.com/smartphone-attacks-rise/
37. Security Service MI5, Interception of Communications | MI5 - The Security Service. Security Service MI5. https://www.mi5.gov.uk/interception-of-communications
38. Fagundes, L.: Smartphone use and data confidentiality. Virtual data rooms. https://www.securedocs.com/blog/2014/05/smartphone-use-and-data-confidentiality