A Social Issue With Smartphones

Seyhmus Yilmaz, Sultan Zavrak, Fatih Kayaalp

Abstract: Today, in many parts of the world, it is becoming more and more widespread for users to be tracked by mobile smart phone platforms. An apparent motive for this is that numerous advertising companies are utilizing smart phone platforms more than they did some time ago. This is a significant area of this study as most users think that being tracked is a big disadvantage in life while others take a different view. Smart phone technologies provide a massive amount of practical features to individuals but at the same time they extremely influence confidentiality of the users. On the other hand, smart phones technologies are not efficient in appropriately communicating confidentiality threats to individuals. Moreover, widespread confidentiality threat communication techniques in smart phone application ecosystems do not consider the real data access behavior of user applications in their threat evaluations. The purpose of this paper is to present some of arguments and considers whether, on balance, it is truly a disadvantage to be tracked by smart phone platforms.

Index Terms: Social issue with smartphone, tracking people, privacy problem.

1 INTRODUCTION

Mobile smart phones have unquestionably brought great advantages to human beings. Nevertheless, it is significant to be aware of the disadvantages of the smart phone platforms as well. People who use smart phones are being tracked by mobile smart phone platforms, applications, games or other kinds of programs on the smart phones. Unique Identifier number for a smart phone, current location and individual information like real name, age, gender can be gathered by some applications [12]. Moreover, it is impossible for us to alter these kinds of tracking methods or deactivate them. Advertising business that employ the data to collect records on smart phone users receive the data regularly from applications. This individual information is being shared broadly and routinely with third-parties. For example, if individuals visited a website such as bbc.co.uk by using our smart phones, 10 different companies such as Microsoft, Google and so on might receive this information about us can be visit within milliseconds [2]. Our visits are logged by these firms immediately. This is becoming a very important issue in people's lives. How is it affecting users? This report is going to examine tracking methods in two areas. First one is in operating systems side especially like Apple and Android (Google). The other one is in applications side. Two big operating systems Apple and Android (Google) will be discussed in this section. Many people are using iPhone as a smart phone. But most people are unaware of its privacy policies. Furthermore, some do not know their behavior and data are being recorded by Apple. For example, your data can be shared by Apple and its partners. They employ this data according to their Privacy Policy. In addition, the users' data might be combined with another data by Apple in order to give and develop their products, services, content, and advertisements [3].

If a user who uses an iPhone register an Apple ID or buys an item or does an internet survey etc., Apple will gather a lot of data from the user such as their name, email address, mobile number, credit card data and so on [3]. Apple not only records the information about the user but also records the information about the family or friends of the user, when the user shares something with them via iPhone or gives an app as a gift or makes an invitation them. Apple can request Social Security number from the users in the United States as well. Individual data can be used by Apple for internal aims like auditing, information analysis, and research to develop its products, services, and its user communications [3]. As we can see, Apple records everything about us without our consent when we use its smart phone. Similarly, according to Android (Google) privacy policies for applications that are generated by third party, app creators are able to add their privacy policies to Google Play with a link [8]. App creators write their privacy policies and Google does not evaluate them [8]. App developers who decide to release their privacy policies have an option that is given by Google. These privacy policies are completely up to app developers. All applications might not have any privacy policies on Google [8]. On the other hand, if there is a privacy policy for an application, it can be found and read these privacy policies on Google. It can be seen from both policies; Android do not protect us from third party applications. Because app developers can write their policies as they wish and they do not have to publish their policies on Google. As a result of this, app developers can fool users easily. Even most people do not read anything about them and just accept term and conditions without looking. But this can cause serious problems for users. For example, these kinds of applications might be able to record every activity of the user such as messages, contact lists, email addresses. After that information can be used against the users. Especially free applications are more likely to be malicious. Another disadvantage of this is that the data collected by both Apple and Google can be stolen by hackers. Google and Apple have been broken several times in the past. In addition to that, people who work for Apple or Google might employ the users' data for their benefits. Such cases happened in the past. For instance, David Braksdale who used to work for Google as an engineer used his position to get some teenagers' information in order to meet them [9]. He met 4 kids by breaking Google privacy policies. Google admitted this case and sacked him. This showed that our privacy can be violated easily. The users' information can be used against them. Smart phones platforms such as Apple and Google develop advertisements but also create vulnerabilities for their users.

- *Seyhmus Yılmaz, Düzce, Turkey, E-mail: seyhmusyilmaz@duzce.edu.tr*
- *Sultan Zavrak, Düzce, Turkey, E-mail: sultanzavrak@duzce.edu.tr*
- *Fatih Kayaalp, Düzce, Turkey, E-mail: fatihkayaalp@duzce.edu.tr*

Fig. 1. *Some current smartphones*

The users often cannot switch off the tracking. Especially applications do not have an option to deactivate the tracking. Users can remove or prevent the tracking on computers but this is usually impossible on smart phones applications. Some people think that people should have an option to disable tracking because they claim that this is not fair. According to the study, IPhone stores the exact locations of the people with time and date stamp [11]. After that this information will be saved to the users' computers as well when they connect their phone with computer [11]. If someone gets the user's smart phone or computer, they can obtain all locations the user visited. Another issue with smart phones is that some applications such as Twitter, Instagram, and Yelp etc. might obtain the users' address book from their phone [10]. According to New York Times, 11 percentages of free applications gather the address book of users in IPhone [10]. Because of this, members of Congress started to discuss this problem after this. Apple does not intentionally gather individual data from people whose age group are less than 13 and if Apple collects any data about such age groups, it will delete them [3]. In my opinion, this age should be 18, because most people are unable to distinguish right from wrong at the age of less than 13. As mentioned before, the former Google engineer abused the data of teenagers who were about 16 years old. A lot of states have conducted investigations about of Google Street View all over the world. The investigations have been increased steadily over time when people realized that it is gathering Wi-Fi information such as name, postcode, telephone number etc. when the Street View cars captured the streets in 2007 [4]. It is said that these cars as seen in Fig. 2 gathered about 200GB of payload information [4]. Federal Communications Commission sued Google for capturing privacy information such as name, email address, phone number and so on without any permission [4]. Before that case, people were unaware of being tracked. Google then admitted that it had collected individual data. As a result of this, Google paid $7 million fine [6].

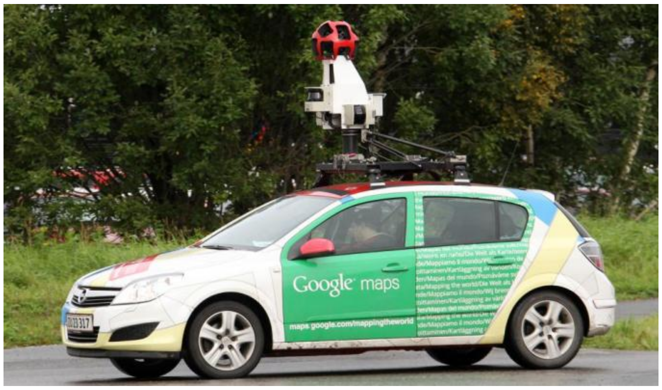


Fig. 2. *Google Street View Car [13]*

For that reasons, tracking people has an adverse impact on our lives. At the beginning of such incidents people had not known that how much privacy information about us mobiles smart phones platforms are tracking. When people have read such papers about this subject they realized that we have no privacy any more. Not just our valuable information but also the information about people we know is being shared all over the world. Now some users feel as if someone would come wherever we go and are watching what we are doing.

2 Behavioral marketing or Targeted advertising

The meaning of this term is to gather and to compile the information about the users such as their behaviors, interests, favorites, and places and so on [5]. In order to produce more accurate profiles, the information can be collected, examined, and combined with data from offline content [5]. After that this data might be employed by advertisements in order to make adverts to a user according to their information that is logged before. For instance, adverts might be shown according to where individual lives or the sorts of applications the users have been interested in [5]. Advertising companies think that these kinds of advertisements serve people to bring their smartphones adverts to people that will probably be affected by the adverts. The third-party cookies that might be employed by advert networks to allow behavioral tracking can be employed by some Smartphone web browsers [5]. The users' mobile phone browsers permit them to disable the third-party cookies. On the other hand, smartphone applications usually don't offer advert network with the capability to set a cookie to trace people [5]. As an alternative, the device identifier of the Smartphone might be used by ad network.

3 Data can be used by Governments

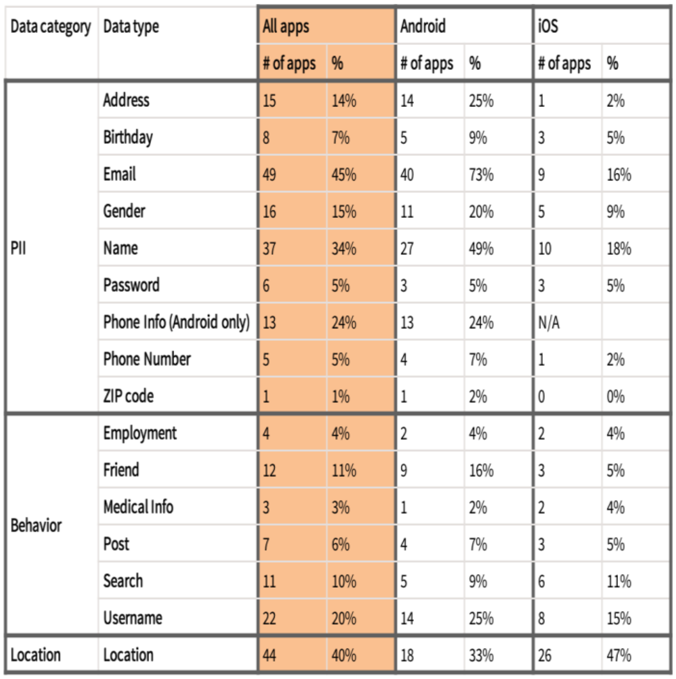
Gathering information about individuals is very beneficial for police or government body. For instance, the place an individual has visited and the thing an individual has done, the time the individual has done particular task. When someone is a suspect, the officers might need to look at what he/she has made and where he/she has visited. These kinds of information about them might be disclosed by their smartphones. As a result of this, the information taken via their Smartphones might be employed against them in a law court [5]. In general, the users' data are preserved by law. On the other hand, the police might be able to use the users' Smartphone information without permission. Some businesses such as Google, Apple have built units to help government and these units are full all the time [10]. In addition, some government bodies built some websites to track people locations [10]. This is entirely dependent on their situation. For instance, the data of Smartphone can be sought by law enforcement; it depends on where the user lives. Locations of smartphones may have been given to police and they can request all location information from the wireless providers in order to trace devices. In addition, all the information of our Smartphone provider has gathered about us can be requested by the police [5]. It is not often clear for Federal privacy laws how simple the police can get information the users' smart phone. This is because the technology is developing at much too fast a pace. A major advantage of this is that law enforcement can catch criminals earlier and can disclose many secrets about criminals. On the other hand, it can be argued that the government bodies can use the data provided by Smartphone against opposition political parties.

4 Conclusion

To sum up, smartphones are growing at much too fast a pace. It ought to be our servant rather than our master. It is essential to control smartphone platforms, before it is too late before they control us. It is advised from this study that if people as voters pressured their governments to make smart phone platforms more responsible and to guard the users from such companies, we could have the advantages of smartphones without their drawbacks.

TABLE 1

Summary of the number of applications in Android and iOS sharing information with third-party domains by data type. Phone info for Android apps only are shown [14].



Data category	Data type	All apps		Android		iOS	
		# of apps	%	# of apps	%	# of apps	%
PII	Address	15	14%	14	25%	1	2%
	Birthday	8	7%	5	9%	3	5%
	Email	49	45%	40	73%	9	16%
	Gender	16	15%	11	20%	5	9%
	Name	37	34%	27	49%	10	18%
	Password	6	5%	3	5%	3	5%
	Phone Info (Android only)	13	24%	13	24%	N/A	
	Phone Number	5	5%	4	7%	1	2%
	ZIP code	1	1%	1	2%	0	0%
Behavior	Employment	4	4%	2	4%	2	4%
	Friend	12	11%	9	16%	3	5%
	Medical Info	3	3%	1	2%	2	4%
	Post	7	6%	4	7%	3	5%
	Search	11	10%	5	9%	6	11%
	Username	22	20%	14	25%	8	15%
Location	Location	44	40%	18	33%	26	47%

References

[1] G. Bal, K. Rannenberg, and J. I. Hong, "Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns," Computers & Security, vol. 53, pp. 187-202, 9// 2015.

[2] A. C. Madrigal, "I'm being followed: How Google and 104 other Companies Are tracking me on the web," The Atlantic, 2012. [Online]. Available: http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/. Last Accessed: Oct. 01, 2016.

[3] Apple Inc, "Privacy," Apple, 2016. [Online]. Available: https://www.apple.com/privacy/. Last Accessed: Oct. 29, 2016.

[4] J. Burt, "Google staff knew street view cars were collecting private data: FCC," Find us on Google+, 2012. [Online]. Available: http://www.eweek.com/c/a/Security/Google-Staff-Knew-Street-View-Cars-Were-Collecting-Private-Data-FCC-276221/. Last Accessed: Oct. 01, 2016.

[5] Privacy Rights Clearinghouse, "Privacy in The Age of The Smartphone," in Privacy Rights Clearinghouse, 2005. [Online]. Available: https://www.privacyrights.org/consumer-guides/privacy-age-smartphone. Accessed: Oct. 01, 2016.

[6] Paul Lilly . (2013). Google Settles Multistate Street View Lawsuit for $7 Million. Available: http://www.maximumpc.com/article/news/google_settles_multistate_street_view_lawsuit_7_million2013. Last accessed 20 March 2013.

[7] M. Liedtke and P. Svensson, "Apple kicks Google Maps off iPhone, adds Facebook", Finance.yahoo.com, 2016. [Online]. Available: http://finance.yahoo.com/news/apple-kicks-google-maps-off-iphone-adds-facebook-211903126--finance.html. Last Accessed: 01- Oct- 2016.

[8] Google. (2013). Privacy Policies for Android Apps Developed by Third Parties. Available: http://support.google.com/googleplay/bin/answer.py?hl=en&answer=2666094. Last accessed 20 March 2013.

[9] Sergio Hernandez. (2010). GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated). Available: http://gawker.com/5637234/. Last accessed 20 March 2013.

[10] Kate Torgovnick. (2012). What data is being collected on you? Some shocking info. Available: http://blog.ted.com/2012/07/24/what-data-is-being-collected-on-you-some-shocking-info/. Last accessed 20 March 2013.

[11] Daily Mail Reporter. (2011). What privacy concerns? iPhone users start posting secret data collected by Apple on Twitter. Available: http://www.dailymail.co.uk/sciencetech/article-1380052/iPhone-users-start-posting-secret-data-collected-

Apple-Twitter.html. Last accessed 20 March 2013.

[12] S. Thurm and Y. I. Kane. (2010). Your Apps Are Watching You. Available: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html. Last accessed 20 March 2013.

[13] Onedio Teknoloji (2015). Google Street View Arabaları Hava Kirliliğini Saptayacak. Available: https://onedio.com/haber/google-sokak-gorunumu-arabalari-hava-kirliligini-saptayacak-555053. Last accessed 10 October 2016.

[14] Technology Science (2015). Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. Available: http://techscience.org/a/2015103001/. Last accessed 20 October 2016.

[15] Gadgets 360 Staff (2015). 10 Smartphones We Loved in 2015. Available: http://gadgets.ndtv.com/mobiles/features/10-smartphones-we-loved-in-2015-778671. Last accessed 20 October 2016.