Hayes, Darren; Cappa, Francesco; Le-Khac, Nhien-An

Article

An effective approach to mobile device management: Security and privacy issues associated with mobile applications

Digital Business

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Hayes, Darren; Cappa, Francesco; Le-Khac, Nhien-An (2020) : An effective approach to mobile device management: Security and privacy issues associated with mobile applications, Digital Business, ISSN 2666-9544, Elsevier, Amsterdam, Vol. 1, Iss. 1, pp. 1-8, https://doi.org/10.1016/j.digbus.2020.100001

This Version is available at:
https://hdl.handle.net/10419/337880

Digital Business 1 (2020) 100001

Contents lists available at ScienceDirect

Digital Business

journal homepage: www.elsevier.com/locate/digbus

An effective approach to mobile device management: Security and privacy issues associated with mobile applications

Darren Hayes [a,*], Francesco Cappa [b,*], Nhien An Le-Khac [c]

[a] Pace University, Seidenberg School of CSIS, New York, NY, USA
[b] LUISS Guido Carli University, Department of Business and Management, Rome, RM, Italy
[c] University College Dublin, School of Computer Science, Dublin, Ireland

ARTICLE INFO

Article history:
Received 2 July 2020
Received in revised form 23 September 2020
Accepted 30 September 2020

Keywords:
Mobile applications
Mobile device management
Mobile forensics
Mobile security
Privacy
IT risk
Big Data

ABSTRACT

Consumers and organizations often rely on permissions requested during the installation of mobile applications (apps) and on official privacy policies to determine how safe an app is and decide whether the app producer is acting ethically or not. This research raises several concerns about the collection and sharing of personal data conducted by mobile apps without the knowledge or consent of the user. The findings of this case study research clearly demonstrate that permissions and privacy policies are not enough to determine how invasive an app is. By analysing six popular mobile apps we demonstrate how extensive amounts of data, which go well beyond the permissions requested of the user, are commonly collected. This study illustrates the effectiveness of our proposed approach, which is based upon a static and dynamic analysis, in addition to a review of privacy policy statements. From a corporate perspective, the outcomes of this study are important to understand how many mobile apps put employees, and intellectual property, at risk. Furthermore, we have highlighted how sensitive information being collected may eventually be used in public or private investigations. Moreover, we have also evidenced how the data being collected is contrary to the developers' privacy policies. The results of this study will assist policymakers who may be concerned with consumer privacy and data collection practices.

1. Introduction

By the third quarter of 2019, there were 1.8 million iOS applications (”apps”) on Apple's App Store and 2.47 million apps on Google Play store (“App store Insights from Appfigures”, 2018; “StatSoft Europe”, 2019). Given the vast selection of mobile apps available, each with varying degrees of security and privacy, it is critical for organizations to understand which mobile apps, being used by their employees, may put their organization at risk, and for individuals to understand what information is being collected.

When these statistics are coupled with the fact that the lines between personal mobile devices and business-owned mobile devices have become blurred, it is increasingly important for organizations to examine mobile apps. In fact, these apps can leak personal data about employees that could be used for social engineering, i.e. the manipulation of individuals to divulge valuable and sensitive data to cyber criminals (Abraham & Chengalur-Smith, 2010; Aldawood & Skinner, 2019; Hayes & Cappa, 2018; Krombholz, Hobel, Huber, & Weippl, 2015; Mouton, Leenen, & Venter, 2016; Salahdine & Kaabouch, 2019), lead to data exfiltration or even be associated with malicious code (malware). Moreover, the use of customer personal data, i.e. personally identifiable information (PII) (Hayes, Cappa, & Cardon, 2018; Vo, Fuhrmann, Fischer-Hellmann, & Furnell, 2019), makes it possible to identify individuals and subsequently social engineer them. Consequently, data collected by mobile apps can put both employees and organizations at risk (Sapountzi & Psannis, 2016; Stavrou & Gritzalis, 2015). Therefore, companies are increasingly concerned about potential cyber-attacks (Bayrak & Brabowski, 2006; Center for strategic international studies McAfee, 2012; Genge, Kiss, & Haller, 2015; Shackelford, 2012), and mobile applications are a component of that cyber threat landscape. Mobile device management (MDM) is an enterprise deployment and management scheme for mobile devices such as cellular telephones and tablets. This scheme is generally comprised of policies and an application, with the latter being used to administer policies that restrict an employee's mobile app installation privileges and enforce security protocols. These restrictions are designed to enforce security updates, reduce the risk of malware, and mitigate the risk of exposing non-public data, including personally identifiable information (PII) and intellectual property (IP). If an employee mobile device is lost or stolen, a mobile device manager, or incident responder, can remotely wipe (delete) data stored on the device. Apple Configurator 2 (Apple, 2020) and Jamf Pro (Jamf, 2020) are two examples of MDM applications. Enterprises are increasingly adopting MDM systems to remotely control and secure the data stored in

* Corresponding authors.
E-mail addresses: dhayes@pace.edu, (D. Hayes), fcappa@luiss.it. (F. Cappa).

http://dx.doi.org/10.1016/j.digbus.2020.100001

employee's mobile devices (Rhee, Jeon, & Won, 2012). Therefore, analysing third party apps from a threat intelligence perspective, to determine security issues, will further aid towards the establishment of better security policies and procedures (Rhee, Won, Jang, Chae, & Park, 2013).

In addition to the security concerns related to the PII of employees collected through mobile apps, there are also threats to national security. The collection of information beyond the consent of the individual represents a privacy concern. In this case there may be no risk to a specific organization - nevertheless there are privacy concerns because the developer's methods of data collection violate their own privacy policies, with the goal of gathering Big Data (Del Vecchio, Di Minin, Petruzzelli, Panniello, & Pirri, 2018; Elia, Polimeno, Solazzo, & Passiante, 2019; Visconti & Morea, 2019). Big Data may generate consumer preferences, thereby producing commercial value (Jin, Wah, Cheng, & Wang, 2015; Johnson, Friend, & Lee, 2017). Therefore, identifying PII collected by a mobile app is also crucial to identifying privacy issues and potential regulatory violations by companies.

Individuals and organizations often rely on requested permissions associated with mobile apps, in addition to official privacy policies, to determine how safe an app is and to determine what information is being collected. However, there are several concerns about the disclosure of data being gathered by these apps, and what PII is collected from individuals without their knowledge or consent (Choe, Jung, Lee, & Fisher, 2013; Thurm & Kane, 2010). Privacy issues arise when the data collected is more than what was expected by the user, thereby increasing security risks for the individual (Ali et al., 2018; Burger, Oz, Kennedy, & Crooks, 2019). While previous studies have analysed privacy issues associated with mobile apps (Hayes, Snow, & Altuwayjiri, 2018; Liu, Gao, & Wang, 2017; Moreno, Serrano, & Fernández-Medina, 2016; Snow, Hayes, & Dwyner, 2016; Vigneri, Chandrashekar, Pefkianakis, & Heen, 2015), it is not yet clear how much they are diffused and the methodology used to effectively examine them. Thus, the research questions that we address in this paper is: What are privacy and security issues associated with certain popular mobile applications, and how data collected can be used by companies, practitioners and policymakers?

This research proposes a series of steps, based on static and dynamic analyses, in addition to a review of privacy policy statements on popular mobile apps. The findings from this research study clearly demonstrate that requested permissions and privacy policies are not enough to determine how invasive an app is in terms of potentially compromised PII. In particular, some app producer claims about location tracking, and the collection of personal information, go far beyond what it is stated in their privacy policies. Organizations, and, more specifically IT risk management, and personnel involved in MDM (Andriotis, Oikonomou, Tryfonas, & Li, 2016; Li, Tryfonas, Russell, & Andriotis, 2016; Rhee et al., 2013), will also benefit from the findings of this research to institute a more comprehensive review of mobile applications, when developing corporate policies and procedures. Furthermore, data collected from mobile apps beyond what is stated in their privacy policies may eventually be used by digital forensics investigators in private and public investigations against criminals. Finally, by illustrating how corporate privacy policies greatly differ from reality may be useful also for policymakers with privacy concerns – especially in the European Union because of the General Data Protection Regulation (GDPR). Therefore, this study contributes to the existing body of academic research on this topic (Hayes & Cappa, 2018; Sapountzi & Psannis, 2016; Stavrou & Gritzalis, 2015) by providing an analytical framework that highlights the steps required to analyze apps and discover privacy issues associated with mobile apps, as well as the possible usage of the information collected.

The structure of this paper is as follows: in Section 2, we provide a background to our research; in Section 3, we have described the methodology used during our experimentation; in Section 4, we present the results of our analyses; and, finally, in Section 5 we discuss our findings and conclude with our contribution to academia and describe the implications for managers and policymakers.

2. Background and literature review

Mobile device usage is increasing exponentially as cellphones become more pervasive globally. In 2011, more than 4 billion mobile-device users were identified and that number has continued to increase in subsequent years (Wamba, Akter, Edwards, Chopin, & Gnanzou, 2015), thereby offering companies the opportunity to collect vast quantities of PII data from mobile apps (Trabucchi, Buganza, & Pellizzoni, 2017; Yaqoob et al., 2016). Consequently, mobile apps are increasingly being downloaded by consumers to purchase products and services for their everyday lives (Furletti, Trasarti, Cintia, & Gabrielli, 2017). In parallel, concerns about the data collected by apps, beyond what is stated in the privacy policy, continue to grow (Moreno et al., 2016). Thus, consumers and organizations are becoming alarmed about how mobile apps are collecting PII (Wijesekera et al., 2015). In terms of information security, there are three main areas of concerns that form the so called C.I.A. triangle: confidentiality, integrity and availability (Chaeikar, Jafari, Taherdoost, & Kar, 2012; Tipton, Forkey, & Choi, 2016; Yin, Fang, Guo, Sun, & Tian, 2020). In this research we have focused on the first dimension, i.e. confidentiality, by analysing a mobile application's access to PII beyond the requested consent.

Mobile apps can collect vast amounts of information, about users for marketing purposes, thereby allowing the collection of Big Data, which is data characterized by high Volume, Variety and Velocity (Ardito, Scuotto, Del Giudice, & Messeni, 2018; Elia et al., 2019; Johnson et al., 2017; Maroufkhani et al., 2019). It can be lucrative for companies collecting Big Data from mobile apps (Erevelles, Fukawa, & Swayne, 2016; Jang & Kwak, 2015). The value of Big Data may prompt mobile app developers to collect more information from individuals than they disclose in their privacy policies, which could be as construed as misleading to consumers. Moreover, the data being collected is often not adequately protected and will therefore expose individuals to the potential risks associated with social engineering (Wijesekera et al., 2015). Additionally, the information being collected without consent raises concerns about the risk for social engineering (Abraham & Chengalur-Smith, 2010; Airehrour, Nair, & Madanian, 2018; Hayes & Cappa, 2018; Krombholz et al., 2015; Mouton et al., 2016), and also the threat of cyber-attacks against corporations (Hayes & Cappa, 2018). The aforementioned considerations call for a deeper understanding of how much data is being collected through mobile apps without user consent and whether the user data is being securely stored.

The research herein contributes to the existing academic literature focusing the analysis of privacy issues associated with mobile apps (Jain & Shanbhag, 2012; Snow et al., 2016; Vigneri et al., 2015; Wang, Duong, & Chen, 2016; Yun, 2013) and highlights the potentially unethical behavior of some companies that collect sensitive PII. For example, recent research has uncovered how Uber tracks user location in ways that contradict their privacy policies (Hayes, Snow, & Altuwayjiri, 2018). Other research has identified how apps, like Angry Birds, could be used by government agencies to profile individuals (Snow et al., 2016). Recently it has been shown that TikTok has been collecting mobile device identifiers for more than a year (Poulsen & McMillan, 2020). Additionally, it has been shown that there are potential security risks associated with third-party geolocation requests from apps (Liu et al., 2017) and many apps connect to known malware server domains (Vigneri et al., 2015). Moreover, Snow et al. disclosed how advertisers and mobile app developers exchange user data (Snow et al., 2016), Vigneri et al. analysed malware activities and tracking websites (Vigneri et al., 2015). In addition, Wang and his research group evaluated consumers' intentions to disclose PII (Wang et al., 2016), while Jain and Shanbhang assessed that unsecured mobile apps can cause serious security issues (Jain & Shanbhag, 2012). Furthermore, Yun and colleagues focused on GPS positioning issues with mobile apps. In our research, we have instead posited a series of steps that allows a comprehensive

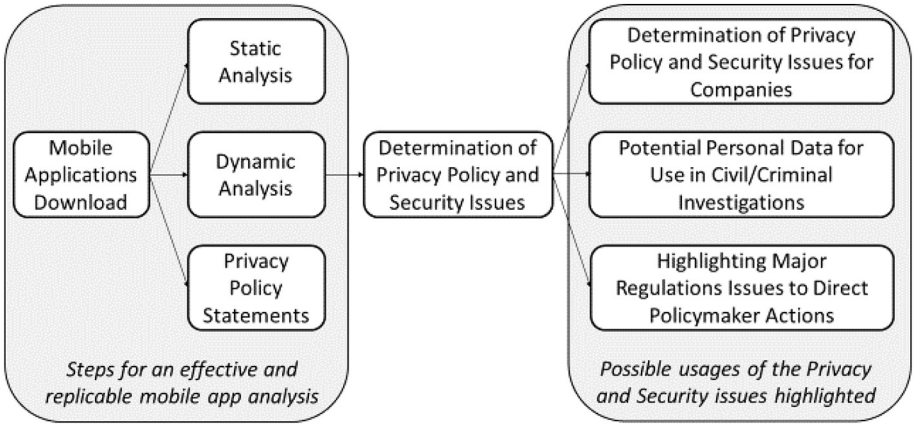

Fig. 1. Research steps proposed in this study based on the integration of static, dynamic and privacy policy statements analyses, and derived outcomes for scholars, practitioners and policymakers.

examination of all the privacy issues associated with mobile apps, and assess the type of data collected without user consent.

More precisely, by performing a static, dynamic and privacy policy statement analyses of mobile apps, as reported in Fig. 1, rather than just relying on one methodology, as illustrated in previous research (Hao, Liu, Nath, Halfond, & Govindan, 2014; Lindorfer, Neugschwandtner, & Platzer, 2015; Uto, 2013; Yan & Yin, 2012), we have illustrated the main threats to individual privacy and organizational security. Our research focuses on a group of mobile apps that are most commonly used by individuals and employees. A thorough analysis of these mobile apps has identified how companies are collecting vast quantities of data about individuals, beyond user consent, which in turn affect individuals' privacy and increases organizational risk, with the added potential for both social engineering and the dissemination of malware. Broadly speaking, our findings can also extend to national security and national policy, as detailed in a recent article that highlighted how fitness apps can be used to track military personnel and military bases (Sly, Lamothe, & Timberg, 2018).

3. Methodology

There were three phases of mobile app analysis conducted in our research, including (1) a static analysis of the mobile app, (2) a dynamic (or behavioral) analysis, and (3) an examination of the mobile app developer's privacy policy.

The mobile apps, selected as relevant cases for this study, were as follows: Tinder, WhosHere, Instagram, Seamless, Bumble and Spotify. Our app selection was based on a survey administered to students enrolled in the Master of Science in Computer Science program, and employees and professors at a university in the United States. We asked survey participants to select the three mobile applications that are amongst the most popular offered, for free, in the USA. Consequently, instead of relying on statistics about the most downloaded mobile apps, we considered mobile apps that would be important in the future and asked which app they think will be the most popular in the future. In addition, we restricted the possible selection of apps to the US market in order to have comparable procedures and obligations for developers, as well as the cultural mind-sets of the targeted users. Using the sample collected, we initially analysed mobile apps from the most cited to the lowest and we concluded the analysis based on theoretical sampling (Eisenhardt & Graebner, 2007; Gilbert, 2005; Gioia, Corley, & Hamilton, 2013), i.e. reaching saturation "when [there are] no significant new insights" (Conlon, Timonen, Elliott-O'Dare, O'Keeffe, & Foley, 2020). Therefore, after having analysed the six most recurrent apps and based on the feedback collected, we determined that we had an adequate amount of data to conclude our study, similar to other studies conducted in the field of computer science (Urquhart, Lehmann, & Myers, 2010).

Although we examined stand-alone mobile apps, in some cases we found that there are partnerships and information sharing with other social media companies. This practice has become a popular concept and is referred to as "deep-linking", whereby a mobile app seamlessly links with another app. Moreover, these mobile apps are cross-platform, i.e. available for both iOS (iPhone/iPad) and Android mobile devices. In our study we focused on analysing the Android version of the app, since this operating system covers almost 90% of the global app market (Cappa, Del Sette, Hayes, & Rosso, 2016). In the following subsections we describe the six apps that were examined for our study, and the methodologies used, i.e. static, dynamic and privacy policy statements analyses.

Tinder

Tinder is a dating app, with an estimated 50 million active users internationally, while the app has approximately 100 million downloads ("Tinder", 2020). Founded in 2012, the company is headquartered in Los Angeles, California. Once the user established a profile on Tinder, he/she is presented with pictures of potential dates (people) that may be a suitable match to the user. If the user likes a particular user profile, then the user will swipe right on the profile; a left finger swipe on a profile indicates that the user dislikes a profile.

WhosHere

WhosHere is a location-based mobile application for finding friends. Stephen Smith and Bryant Harris founded the company in 2008. WhosHere has more than 10 million app users globally seeking to make connections with local people ("WhosHere", 2020). The app allows users to connect with others in close proximity, via text, calls and video or through use of a smartphone's GPS function.

Instagram

Instagram is an online photo-sharing application and social network platform ("Instagram", 2020), which was launched in October 2010 and was later acquired by Facebook in 2012. Instagram allows users to both edit and upload photos and short videos through a mobile app. Users also have the ability to add captions to their posts and include hashtags and geotags to index their posts. Each user post displays on their followers' Instagram feeds and can also be viewed by the public when tagged using hashtags or geotags. Users also have the option of making their profile private so that only their followers can view their posts. Instagram is not only a tool for individuals, but also for businesses. In fact, the photo-sharing app offers companies the opportunity to start a free business account to promote their brand and products.

Seamless

Based in New York City, the Seamless company was established in 1999 by Jason Finger and Paul Appelbaum ("Seamless", 2020). The mobile app enables consumers to order food for delivery or order takeout food. In

2017, the company processed close to 400,000 orders daily and realized almost $4 billion in gross sales, and it has more than one million downloads.

Spotify

Based in Stockholm, Sweden, the company was founded by Daniel Ek and Martin Lorentzon in 2008 ("Spotify", 2020). Spotify is a digital music, podcast and video streaming company with more than 70 million paid subscribers worldwide. There are both a pay per use and free versions of the app available, but the features are the same with the exception of the advertising presence or not.

Bumble

Based in Austin, Texas, the company was founded by Whitney Wolfe, the co-founder of Tinder, in 2014. Bumble is a dating and social media app with location-based tracking built in. The mobile app has approximately 23 million registered users ("Bumble", 2020).

3.1. Static analysis

The initial analysis conducted on the aforementioned mobile apps was a static analysis, which involved (a) reverse-engineering the code encapsulated in the mobile application and (b) a review of the application SQLite database, including its structure and content. The rationale for reverse engineering the code was to identify the permissions that the application sought to establish and then subsequently identify if any of these permissions potentially violated the application developer's privacy policy disclosed to the user. Furthermore, we sought to assess if any of the requested permissions were moderate to high risk, thereby posing a threat to the individual and eventually her/his respective organization. Our static analysis included a review of the Android application package (APK) file and this code review provided the app manifest, which included the application permissions. An app manifest can include location-tracking permissions, based on cell sites (cell towers or antennae) or user location based on proximity to access points (Wi-Fi connections). In addition, a manifest can include permissions that extend to the activation of a user's device microphone or even manipulate files on a computer that the mobile device synchronizes to. There are numerous tools available for examining the code in an APK, including dex2jar and FileViewer Plus. During our analysis, we used an online Java-based APK decompiler application (Java Decompilers, 2018). The rationale for selecting this tool to decompile the APK was that we were not required to download this decompiler and could simply upload the APK file online, thereby mitigating the risk of a malware infection to our computer from an unknown source.

As previously mentioned, the static analysis also included a review of the mobile app's SQLite database. Virtually every mobile app on a smartphone, or tablet, stores information in a relational database called a SQLite database. Each database is comprised of tables that are linked. Each table has rows and columns – similar to Microsoft Excel. The Facebook app, for example, maintains a SQLite database. Within that database, one table may contain the user profile, while another table may contain the user's Facebook friends, and another table can contain Facebook Messenger chats. All tables in the SQLite database are linked by a key, as is the case with any relational database, to maintain referential integrity. Ultimately, it is up to the developer to decide what information, contained in each table of the SQLite database, should be encrypted. All information in these tables should be encrypted: (1) on the device, (2) during transmission and (3) at rest on the company's server, to protect the user. Encryption is a critical component of effective security protocols, and, if it is not implemented by app developers, it puts both the user and the organization at risk.

3.2. Dynamic analysis

The second step that we conducted was a dynamic analysis, which involves a behavioral analysis of the mobile application, once it is executed (Hao et al., 2014; Lindorfer et al., 2015; Yan & Yin, 2012). Unlike a static analysis of the code, which provides limited information about network connections, a dynamic analysis can provide detailed information about network connections that an application can make during its usage. This is important in ascertaining where geographically user information is being transmitted to and also if there are connections to servers that pose a risk to the organization; one mobile application can literally connect to hundreds of servers domestically and internationally. For example, some server connections could be associated with the distribution of malware, while other mobile application communications may proxy through servers in countries associated with state-sponsored theft of intellectual property.

3.3. Privacy policy analysis

Finally, we analysed the privacy policy statements disclosed by each company to the general public. There is no single federal privacy law in the United States that requires companies to have a privacy law posted on their website. Nevertheless, existing state and federal laws, like the Consumer Credit Reporting Control Act (Consumer Credit Reporting Control Act Public Law, 1970) or the CalOPPA (California Online Privacy Protection Act) (California Online Privacy Protection Act, 2003), suggest that companies should provide a written privacy policy about PII that they collect and how they share these data with third-parties. However, with the exception of personal healthcare information, which is protected under HIPAA (Health Insurance Portability and Accountability Act) (Health Insurance Portability and Accountability Act (HIPAA), 1996), consumers are limited in what PII they can prevent being shared. Thus, we carefully examined the privacy policy of the mobile apps considered in this study to identify whether they comprehensively disclose all the data that they collect.

4. Results

In this section, we outline the findings from the analyses conducted on each of the six mobile apps examined with the steps proposed in this study, as reported in Fig. 1. Our research findings clearly indicate that each of these major apps expose individuals to some type of privacy issue that was not clearly stated in their privacy policy. The outcomes are reported in the following paragraphs discerning each app one by one.

4.1. Tinder

The Tinder app utilizes a customer's location to determine potential matches within the vicinity of the user. However, the app stores user location information in plaintext on the device without disclosing this to the customer, which is both a security vulnerability and a privacy concern. The Tinder app also uses deep-linking to connect to the Spotify app if the user also has Spotify installed on his device. We observed this connection, during our static analysis of the Tinder app SQLite database, which contained the Spotify user ID and Spotify playlist. It appears that Tinder utilizes a user's music playlist, from Spotify, to improve its algorithm that matches people together. Information about this deep-linking, between Tinder and Spotify, is not available to users of the Tinder app, who review the company's privacy policy. This represents a concern for the user and how they are being profiled by Tinder.

The Tinder app also uses Taplytics, which is a mobile app analytics company (Taplytics Inc., 2018). Within the SQLite database for Tinder, in the Taplytics table we identified the following PII: birthday, city, country, county, data provider, gender, language, location radius, device model, operating system version, and age. Interestingly, we determined that this information could only have come from the user's Facebook account, as it is not information directly obtained from the user; in fact, the Facebook app was also installed on the mobile device used in our experimentation. Once again, the deep-linking transactions and PII data collected are not disclosed in the company's privacy policy.

4.2. WhosHere

The WhosHere app, continually requests the user's location. Moreover, the extent to which this location information is requested and stored in plaintext is perhaps a concern for consumers. For example, if the user loses her/his smartphone and a hacker can unlock the device, then the WhosHere data is readily available in an unencrypted format. It appears that the timestamps saved in the WhosHere app relate to when the user opened and closed the app. The app also captures the device GUID (Globally Unique Identifier), which is a concern, as we did not find any reference to the GUID capture in the company's privacy policy.

4.3. Instagram

We determined that Instagram captures the profile and images of connected Instagram users locally on the device. Many of these profiles are associated with a URL that can be clicked and viewed in a web browser. Some of the URLs provided an "Access Denied" message while other profiles were readily accessible in a web browser. The accessible URLs displayed chat from other Instagram users. If an Instagram user is logged into Facebook, then the user's activity is also logged in the Facebook account. However, these exchanges of PII, between these apps, could not be found in the app developer's online privacy policy statement. We also identified numerous web links, in the user profile, to third-party advertisers.

4.4. Seamless

The Seamless app integrates with the Facebook app and therefore there is sharing of information across these apps, without the user's consent or knowledge. During our static analysis of the Seamless app SQLite database, we noted that the app encrypts the user's data. This demonstrates that their developers have instituted good security protocols, unlike the other mobile apps that we have researched. Our dynamic analysis revealed that Seamless uses an analytics company called UA Analytics for user analytics. Seamless also utilizes Google Analytics and shares information that includes user restaurant searches, ratings and reviews, orders and app login data. Seamless also utilizes Taplytics, although it is unclear what information is shared since the data stored within the Taplytics table, in the Seamless database, was encrypted. Seamless also uses a company called Apptimize to perform constant testing of its app. The Seamless app also uses Branch Metrics and Crashlytics to collect additional user analytics. With regards to hosting and advertising support, our dynamic analysis identified that Seamless uses Amazon and Yahoo!. None of these aforementioned third-parties were disclosed in the privacy policies that we reviewed, thereby raising concerns about the personal data that is being shared with third-party companies.

4.5. Spotify

Our static analysis showed that the SQLite database, for the Spotify app, contained user data that was unencrypted. In addition, we have discovered numerous web links to profiles that contained the URL "fbcdn.net", i.e. Facebook profiles, which possibly demonstrates how Facebook is collecting user data without explicit consent. Unsurprisingly, the SQLite database stores user playlists, which include pictures of artists and album covers. Unfortunately, the username and email address for the Spotify user are stored on the smartphone device in plaintext. Moreover, user activity and the user's Twitter connections are stored in the Spotify SQLite database in plaintext. In summary, the Spotify app stores the username, email address used to register for Spotify, playlists, web links to Facebook profiles and Twitter connections in plaintext, which represents clearly a security concern.

During our dynamic analysis of the Spotify app, we identified that the company uses Crashlytics and Adjust Analytics for gathering analytical data from its users. We also noted connections to servers operated by Amazon AWS and to Akamai Technologies, who provide hosting to Spotify, which occur without the users' knowledge. Overall, the PII collected and stored, by the Spotify app, appear to go well beyond the company's privacy policy, which is a privacy concern for consumers.

4.6. Bumble

During our static analysis of the Bumble app SQLite database, we found that the user data, which included names, addresses, interests, locations and photos, were all unencrypted, i.e. visible in plaintext. Again, this raises security concerns for users and corporations, especially as they are not aware of such data collection. Finally, from our dynamic analysis, we evidenced that the Bumble app also shares user data with other third-party companies for analytics, i.e. Google Analytics and Apps Flyer. The mobile app also saves the profile details of the users on the app, along with their profile images and other social network profile links. It was interesting to note with our dynamic analysis how the Bumble app also connects to servers operated by both Facebook and Microsoft, in addition to servers owned and operated by Bumble.

5. Discussion

With an increasing emphasis on the benefits brought about by Big Data, interest in acquiring PII data continues to grow unabated (Alharthi, Krotov, & Bowman, 2017). In fact, Big Data represents an important source of information to understand consumer sentiment and make business decisions based on emerging trends, in an effort to gain competitive advantage (Acquaviva et al., 2019; Berthon, Pitt, Kietzmann, & McCarthy, 2015; Del Vecchio, Mele, Ndou, & Secundo, 2018; George, Haas, & Pentland, 2014; Johnson et al., 2017; Kim, Jung, Chang, & Choi, 2019; Marshall, Mueck, & Shockley, 2015; Mazzei & Noble, 2017; Paniagua, Korzynski, & Mas-Tur, 2017; Pilloni, 2018; Rindfleisch, O'Hern, & Sachdev, 2017; Visconti & Morea, 2019). In fact, mobile apps have the potential to provide companies more detailed PII than any other source, primarily because of deep-linking to other mobile apps (De Angelis & Di Marzo Serugendo, 2017), and also because of their intense daily usage by the general public (Furletti et al., 2017). Mobile apps can acquire other device data using a variety of permissions; data that can include the device name, operating system, user location, microphone and camera. Increasingly, apps are collecting data also beyond what is stated in their privacy terms, while simultaneously collecting Big Data. Furthermore, the collection of information beyond user consent also represents a legitimate concern for organizations. Employee PII can be used to social engineer people (Abraham & Chengalur-Smith, 2010; Airehrour et al., 2018; Hayes & Cappa, 2018; Krombholz et al., 2015; Mouton et al., 2016) and also serve as a medium to launch cyber-attacks (Hayes & Cappa, 2018). Consequently, companies use MDM to restrict app installation so as to reduce security risks. However, as employees increasingly use their own mobile devices at work and in their everyday life, it is important for organizations to understand mobile app permissions and the PII collection methods employed by developers.

There is growing scholarly interest in understanding the extent to which mobile apps collect PII (Jain & Shanbhag, 2012; Snow et al., 2016; Vigneri et al., 2015; Wang et al., 2016; Yun, 2013). Consequently, focusing on the "confidentiality" aspect of the C.I.A. triangle for determining concerns in the context of information security (Chaeikar et al., 2012; Tipton et al., 2016; Yin et al., 2020), this study analysed six free popular mobile apps in the USA to determine the extent to which data collected goes beyond the company's publicly stated privacy policies. The study highlighted how it is possible to determine how PII is being collected without user consent. These outcomes are extremely relevant for organizational information security personnel and as a means to mitigate information technology (IT) risk.

Using the steps proposed in this research, and reported in Fig. 1, we have first demonstrated how it is possible to comprehensively and effectively analyze the information collected by popular apps, and then also illustrated how this information can be utilized. In particular, we have proved how PII is being collected without being disclosed in the company's

privacy terms and without user consent in many cases. More specifically, we have described how apps, like Tinder, Spotify, Seamless and Instagram, gather information from other mobile apps and user social media accounts. This is a concern for users, especially given that all of this information is being shared with third-party providers. Moreover, other apps like WhosHere, Tinder, Bumble, Spotify and Instagram collect information, without user consent; this data includes geolocation data and GUID, which is stored locally in an unencrypted format. Finally, some apps, including Spotify, Bumble, Tinder and Seamless, share personal data with third parties, like Taplytics, App Flyer, Crashlytics, Adjust Analytics, and Google Analytics, without user consent.

Our reported findings were made possible using both a static and a dynamic analysis, and by examining privacy policies, rather than just relying on one or two methods of examination, as noted in previous studies (Hao et al., 2014; Lindorfer et al., 2015; Uto, 2013; Yan & Yin, 2012). The first contribution of this study is the empirical evidence pointing to the fact that app developers go well beyond their stated claims about personal data collection (see Fig. 1). Thus, we contribute to the academic body of literature by providing empirical evidence for the efficacy of our methodology.

A second contribution of this research is the evaluation of organizational IT risk associated with popular mobile apps, which is largely the result of the collection of PII, third party sharing of this data and the unencrypted storage of personal data. With so much PII data being collected, without personal consent or knowledge, this is also a major concern for an individual's privacy. More specifically, organizations should devote greater attention to this issue and determine proper organizational policies to mitigate risks to employees, including social engineering, while preventing the theft of corporate intellectual property. PII information, leaked by mobile apps, could be used to uncover corporate secrets or even to social engineer people (Abraham & Chengalur-Smith, 2010; Hayes & Cappa, 2018; Krombholz et al., 2015; Mouton et al., 2016). Given the growing importance of MDM (Rhee et al., 2012; Rhee et al., 2013), while considering the recent increase in telecommuting, in addition to organizational support for bring your own device (BYOB) (Steiner, 2014), the findings in the research will serve to enhance the security posture of companies and contribute to the academic body of knowledge related to organizational security.

Moreover, we have also outlined the potential use of PII and illustrated the security risks that can be revealed using our novel approach, as reported in Fig. 1. The fact that virtually no data stored locally, about the user, was being encrypted means that law enforcement can use digital forensics tools, including the aforementioned tools for private and public investigations (Cappa et al., 2016; Farjamfar, Abdullah, Mahmod, & Udzir, 2014). Thus, a third contribution of this study is the contention that, in addition to determining the threats to both companies and individuals, data collected by mobile apps can be also used in criminal and civil investigations (Hayes, Cappa, & Cardon, 2018). For example, an investigator can quickly ascertain what social media accounts a suspect maintains because of deep-linking, as noted through our experimentation earlier. Furthermore, the outcomes of this study can be relevant also for policymakers and regulatory bodies. Indeed, the evidence that mobile apps are effectively collecting information beyond user consent is a cause for concern to organizations and individuals, while highlighting the urgency for countermeasures. Moves to mitigate and prevent such misconduct should represent a priority for policymaking. The benefits for acting in this capacity would mitigate corporate risk, while reducing the privacy concerns of the general public.

The aforementioned contributions of this study, for the academic community, practitioners and policymakers related to identifying privacy and security issues, in addition to the PII that may be collected, are summarized in Fig. 1, in the form of an analytical framework (Hayes, Cappa, & Cardon, 2018).

6. Conclusions

This research illustrates why there are growing concerns about privacy, related to mobile apps, and continues to attract the attention of academia, politicians and corporate management (Al-Muhtadi, Shahzad, Saleem, Jameel, & Orgun, 2019; Hooper & McKissack, 2016; Loreti, Bracciale, & Caponi, 2018; Papageorgiou et al., 2018; Shackelford, 2016; Wang et al., 2019), while this study will create a better understanding of the issues at hand. The results of this study are important for scholars, companies, practitioners and policymakers, and lay the groundwork for future studies on this topic.

We anticipate that further research will be conducted in this area. First, this study was conducted on six mobile apps, as they represent relevant case studies due to their diffusion, popularity and the theoretical sampling procedure. However, future studies should seek to look at other major apps within and outside USA to further analyze how PII is being collected and shared, in order to increase the generalizability of the results, find additional evidence of risk or concern, and also compare privacy and security issues between countries. Another promising research direction should consider an analysis of DNS (server) connections to identify if an app connects to known malware sites or servers that have poor security protocols, e.g. inferior encryption or an expired certificate. Furthermore, although there is great concern about the possible benefits spawning from the collection of Big Data from customers, future research should also try to more definitively assess the value of Big Data connected to each type of data point collected, without user consent. Moreover, while we have focused on a limited sample of USA-based mobile apps, future studies may enlarge the number of apps and countries considered to further validate the results and outline eventual differences that may arise.

Author contributions

Conceptualization, Darren Richard Hayes, Francesco Cappa and Nhien-An Le-Khac; Data curation, Darren Richard Hayes and Nhien-An Le-Khac; Methodology, Darren Richard Hayes and Francesco Cappa; Supervision, Darren Richard Hayes; Writing – original draft, Darren Richard Hayes, Francesco Cappa and Nhien-An Le-Khac; Writing – revision, Darren Richard Hayes and Francesco Cappa.

Declaration of Competing Interest

The authors declare no conflict of interest.

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*, 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001.

Acquaviva, A., Apiletti, D., Attanasio, A., Baralis, E., Bottaccioli, L., Cerquitelli, T., ... Patti (2019). Forecasting heating consumption in buildings: A scalable full-stack distributed engine. *Electronics*, *8*, 491. https://doi.org/10.3390/electronics8050491.

Airehrour, D., Nair, N. V., & Madanian, S. (2018). Social engineering attacks and countermeasures in the New Zealand Banking system: Advancing a user-reflective mitigation model. *Information*, *9*, 110. https://doi.org/10.3390/info9050110.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Futur. Internet*. https://doi.org/10.3390/fi11030073.

Alharthi, A., Krotov, V., & Bowman, M. (2017). Addressing barriers to big data. *Business Horizons*, *60*, 285–292. https://doi.org/10.1016/j.bushor.2017.01.002.

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. J. P. C. (2018). Privacy and security issues in online social networks. *Futur. Internet*(12), 114. https://doi.org/10.3390/fi10120114.

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal*, *25*, 315–329. https://doi.org/10.1177/1460458217706184.

Andriotis, P., Oikonomou, G., Tryfonas, T., & Li, S. (2016). Highlighting relationships of a smartphone's social ecosystem in potentially large investigations. *IEEE Trans. Cybern.*, *46*, 1974–1985. https://doi.org/10.1109/TCYB.2015.2454733.

App store Insights from Appfigures [WWW Document] (2018). appfigures. https://blog.appfigures.com/ios-developers-ship-less-apps-for-first-time/ (accessed 4.28.18).

Apple (2020). Apple Configurator 2 [WWW Document]. https://apps.apple.com/it/app/apple-configurator-2/id1037126344?mt=12 (accessed 7.2.20).

Ardito, L., Scuotto, V., Del Giudice, M., & Messeni, A. (2018). A bibliometric analysis of research on Big Data analytics for business and management. *Management Decision*, *57*, 1993–2009. https://doi.org/10.1108/MD-07-2018-0754.

Bayrak, T., & Brabowski, M. R. (2006). Critical infrastructure network evaluation. *The Journal of Computer Information Systems*, *46*, 67–86. https://doi.org/10.1080/08874417.2006.11645900.

Berthon, P., Pitt, L., Kietzmann, J., & McCarthy, I. P. (2015). CGIP: Managing consumer-generated intellectual property. *California Management Review*, *57*, 43–62. https://doi.org/10.1525/cmr.2015.57.4.43.

Bumble [WWW Document] (2020). https://bumble.com/it/ (accessed 4.29.18).

Burger, A., Oz, T., Kennedy, W. G., & Crooks, A. T. (2019). Computational social science of disasters: Opportunities and challenges. *Futur. Internet*. https://doi.org/10.3390/fi11050103.

California Online Privacy Protection Act, 2003.

Cappa, F., Del Sette, F., Hayes, D., & Rosso, F. (2016). How to deliver open sustainable innovation: An integrated approach for a sustainable marketable product. *Sustainability*, *8*, 1341. https://doi.org/10.3390/su8121341.

Center for strategic international studies McAfee (2012). *In the dark: Crucial industries confront cyberattacks*.

Chaeikar, S. S., Jafari, M., Taherdoost, H., & Kar, N. S. C. (2012). Definitions and criteria of CIA security triangle in electronic voting system. *International Journal of Advanced Computer Science and Information Technology*, *1*, 14–24.

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. *Lecture notes in computer science* (pp. 74–91). https://doi.org/10.1007/978-3-642-40477-1_5.

Conlon, C., Timonen, V., Elliott-O'Dare, C., O'Keeffe, S., & Foley, G. (2020). Confused about theoretical sampling? Engaging theoretical sampling in diverse grounded theory studies. *Qualitative Health Research*, *30*, 947–959. https://doi.org/10.1177/1049732319899139.

Consumer Credit Reporting Control Act Public Law, 1970.

De Angelis, F., & Di Marzo Serugendo, G. (2017). SmartContent—Self-protected context-aware active documents for mobile environments. *Electronics*, *6*, 17. https://doi.org/10.3390/electronics6010017.

Del Vecchio, P., Di Minin, A., Petruzzelli, A. M., Panniello, U., & Pirri, S. (2018). Big data for open innovation in SMEs and large corporations: Trends, opportunities, and challenges. *Creativity and Innovation Management*, *27*, 6–22. https://doi.org/10.1111/caim.12224.

Del Vecchio, P., Mele, G., Ndou, V., & Secundo, G. (2018). Creating value from social big data: Implications for smart tourism destinations. *Information Processing and Management*, *54*, 847–860. https://doi.org/10.1016/j.ipm.2017.10.006.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *The Academy of Management Journal*, *50*, 25–32. https://doi.org/10.5465/AMJ.2007.24160888.

Elia, G., Polimeno, G., Solazzo, G., & Passiante, G. (2019). A multi-dimension framework for value creation through big data. *Industrial Marketing Management*. https://doi.org/10.1016/j.indmarman.2019.08.004 In press..

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research*, *69*, 897–904. https://doi.org/10.1016/j.jbusres.2015.07.001.

Farjamfar, A., Abdullah, M. T., Mahmod, R., & Udzir, N. I. (2014). A review on mobile device's digital forensic process models. *Research Journal of Applied Sciences, Engineering and Technology*, *8*, 358–366.

Furletti, B., Trasarti, R., Cintia, P., & Gabrielli, L. (2017). Discovering and understanding city events with big data: The case of Rome. *Information*, *8*. https://doi.org/10.3390/info8030074.

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, *10*, 3–17. https://doi.org/10.1016/j.ijcip.2015.04.001.

George, G., Haas, M., & Pentland, A. (2014). Big Data and management. *The Academy of Management Journal*, *57*, 321–326. https://doi.org/10.5465/amj.2014.4002.

Gilbert, C. G. (2005). Unbundling the structure of inertia: Resource versus routine rigidity. *The Academy of Management Journal*, *48*, 741–763. https://doi.org/10.5465/AMJ.2005.18803920.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*, 15–31. https://doi.org/10.1177/1094428112452151.

Hao, S., Liu, B., Nath, S., Halfond, W. G. J., & Govindan, R. (2014). PUMA: Programmable UI-automation for large-scale dynamic analysis of mobile apps. *12th annu. int. conf. mob. syst. appl. serv* (pp. 204–217). https://doi.org/10.1145/2594368.2594390.

Hayes, D., & Cappa, F. (2018). Open source intelligence for risk assessment. *Business Horizons*, *61*, 689–697. https://doi.org/10.1016/j.bushor.2018.02.001.

Hayes, D., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information*, *9*, 186. https://doi.org/10.3390/info9080186.

Hayes, D., Snow, C., & Altuwayjiri, S. (2018). A dynamic and static analysis of the uber mobile application from a privacy perspective. *International Journal of Applied Information Systems*, *11*, 11–22.

Health Insurance Portability and Accountability Act (HIPAA) (1996). *United States Congress*.

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*, 585–591. https://doi.org/10.1016/j.bushor.2016.07.004.

Instagram [WWW Document] (2020). https://www.instagram.com/?hl=it (accessed 4.29.18).

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*, 28–33. https://doi.org/10.1109/MITP.2012.72.

Jamf (2020). Jamf pro [WWW document]. https://www.jamf.com/products/jamf-pro/.

Jang, Y. -J., & Kwak, J. (2015). Digital forensics investigation methodology applicable for social network services. *Multimedia Tools and Applications*, *74*, 5029–5040. https://doi.org/10.1007/s11042-014-2061-8.

Java Decompilers (2018). Decompilers online. [WWW document] URL www.javadecompilers.com/apk.

Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and challenges of big data research. *Big Data Research*, *2*, 59–64. https://doi.org/10.1016/j.bdr.2015.01.006.

Johnson, J. S., Friend, S. B., & Lee, H. S. (2017). Big data facilitation, utilization, and monetization: Exploring the 3Vs in a new product development process. *Journal of Product Innovation Management*, *34*, 640–658. https://doi.org/10.1111/jpim.12397.

Kim, Jung, Chang, & Choi (2019). Intelligent micro energy grid in 5G era: Platforms, business cases, testbeds, and next generation applications. *Electronics*, *8*, 468. https://doi.org/10.3390/electronics8040468.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005.

Li, S., Tryfonas, T., Russell, G., & Andriotis, P. (2016). Risk assessment for Mobile systems through a multilayered hierarchical Bayesian network. *IEEE Transactions Cybernetics*, *46*, 1749–1759. https://doi.org/10.1109/TCYB.2016.2537649.

Lindorfer, M., Neugschwandtner, M., & Platzer, C. (2015). MARVIN: Efficient and comprehensive mobile app classification through static and dynamic analysis. *Proceedings - International computer software and applications conference* (pp. 422–433). https://doi.org/10.1109/COMPSAC.2015.103.

Liu, D., Gao, X., & Wang, H. (2017). Location privacy breach: Apps are watching you in background. *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 2423–2429). IEEE. https://doi.org/10.1109/ICDCS.2017.227.

Loreti, P., Bracciale, L., & Caponi, A. (2018). Push attack: Binding virtual and real identities using mobile push notifications. *Future Internet*, *10*, 13. https://doi.org/10.3390/fi10020013.

Maroufkhani, P., Wagner, R., Wan Ismail, W. K., Baroto, M. B., Nourani, M., Maroufkhani, P., ... Nourani, M. (2019). Big Data Analytics and Firm Performance: A Systematic Review. *Information*, *10*, 226. https://doi.org/10.3390/info10070226.

Marshall, A., Mueck, S., & Shockley, R. (2015). How leading organizations use big data and analytics to innovate. *Strategy & Leadership*, *43*, 32–39. https://doi.org/10.1108/SL-06-2015-0054.

Mazzei, M. J., & Noble, D. (2017). Big data dreams: A framework for corporate strategy. *Business Horizons*, *60*, 405–414. https://doi.org/10.1016/j.bushor.2017.01.010.

Moreno, J., Serrano, M. A., & Fernández-Medina, E. (2016). Main issues in Big Data security. *Future Internet*, *8*. https://doi.org/10.3390/fi8030044.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. https://doi.org/10.1016/j.cose.2016.03.004.

Paniagua, J., Korzynski, P., & Mas-Tur, A. (2017). Crossing borders with social media: Online social networks and FDI. *European Management Journal*, *35*, 314–326. https://doi.org/10.1016/j.emj.2016.09.002.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, *6*, 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522.

Pilloni, V. (2018). How data will transform industrial processes: Crowdsensing, crowdsourcing and big data as pillars of industry 4.0. *FuturE Internet*, *10*, 24. https://doi.org/10.3390/fi10030024.

Poulsen, K., & McMillan, R. (2020). TikTok tracked user data using tactic banned by Google. *Wall Street Journal, August*.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, *6*, 353–358.

Rhee, K., Won, D., Jang, S. -W., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *Electronic Commerce Research*, *13*, 243–256. https://doi.org/10.1007/s10660-013-9121-4.

Rindfleisch, A., O'Hern, M., & Sachdev, V. (2017). The digital revolution, 3D printing, and innovation as data. *Journal of Product Innovation Management*, *34*, 681–690. https://doi.org/10.1111/jpim.12402.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*, 89. https://doi.org/10.3390/fi11040089.

Sapountzi, A., & Psannis, K. E. (2016). Social networking data analysis tools & challenges. *Future Generation Computer Systems*, *86*, 893–913. https://doi.org/10.1016/j.future.2016.10.019.

Seamless [WWW Document] (2020). https://www.seamless.com/ (accessed 4.29.18).

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*, 349–356. https://doi.org/10.1016/j.bushor.2012.02.004.

Shackelford, S. J. (2016). Business and cyber peace: We need you! *Business Horizons*, *59*, 539–548. https://doi.org/10.1016/j.bushor.2016.03.015.

Sly, L., Lamothe, D., & Timberg, C. (2018). *U.S. military reviewing its rules after fitness trackers exposed sensitive data*. Washington Post.

Snow, C., Hayes, D., & Dwyner, C. (2016). Leakage of geolocation data by mobile ad networks. *Journal of Information Security and Applications and Research*, *9*, 24–33.

Spotify [WWW Document] (2020). https://www.spotify.com/it/ (accessed 4.29.18).

StatSoft Europe [WWW Document] (2019). https://www.statsoft.de/en/home (accessed 12.13.19).

Stavrou, V., & Gritzalis, D. (2015). Introduction to social media investigation – A hands-on approach, Jennifer Golbeck, Elsevier Publications, USA (2015). *Computers & Security*, *55*, 128–129. https://doi.org/10.1016/j.cose.2015.08.002.

Steiner, P. (2014). Going beyond mobile device management. *Computer Fraud & Security*(4), 19–20. https://doi.org/10.1016/S1361-3723(14)70483-X.

Taplytics Inc (2018). Taplytics [WWW document]. https://taplytics.com/what-is-taplytics.

Thurm, S., & Kane, Y. I. (2010). Your apps are watching you. *Wall Street Journal, December*.

Tinder [WWW Document] (2020). https://tinder.com/?lang=it (accessed 4.29.18).

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and C.I.A. triangle. *Journal of Medical Systems*, *40*, 100–108. https://doi.org/10.1007/s10916-016-0465-x.

Trabucchi, D., Buganza, T., & Pellizzoni, E. (2017). Give away your digital services. *Research Management*, *60*, 43–52. https://doi.org/10.1080/08956308.2017.1276390.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the "theory" back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal*, *20*, 357–381. https://doi.org/10.1111/j.1365-2575.2009.00328.x.

Uto, N. (2013). A methodology for retrieving information from malware encrypted output files: Brazilian case studies. *Future Internet*, *5*, 140–167. https://doi.org/10.3390/fi5020140.

Vigneri, L., Chandrashekar, J., Pefkianakis, I., & Heen, O. (2015). *Taming the Android appstore: Lightweight characterization of Android applications (No. arXiv:1504.06093)*.

Visconti, R. M., & Morea, D. (2019). Big data for the sustainability of healthcare project financing. *Sustainability*, *11*, 3748. https://doi.org/10.3390/su11133748.

Vo, T. H., Fuhrmann, W., Fischer-Hellmann, K. P., & Furnell, S. (2019). Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. *Future Internet*, *11*, 116. https://doi.org/10.3390/fi11050116.

Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How "big data" can make big impact: Findings from a systematic review and a longitudinal case study. *International Journal of Production Economics*, *165*, 234–246. https://doi.org/10.1016/j.ijpe.2014.12.031.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*, 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003.

Wang, Y., Zheng, N., Xu, M., Qiao, T., Zhang, Q., Yan, F., & Xu, J. (2019). Hierarchical identifier: Application to user privacy eavesdropping on mobile payment app. *Sensors (Switzerland)*. https://doi.org/10.3390/s19143052.

WhosHere [WWW Document] (2020). http://whoshere.net/ (accessed 4.29.18).

Wijesekera, P., Baokar, A., Hosseini, A., Serge, E., Wagner, D., & Beznosov, K. (2015). Android permissions remystified: A field study on contextual integrity. *24th USENIX security symposium* (pp. 499–514) Washington, D.C..

Yan, L. K. L., & Yin, H. (2012). Droidscope: seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis. *Proc. 21st USENIX secur. symp. 29*.. https://doi.org/10.1016/B978-1-59749-305-5.00006-2.

Yaqoob, I., Hashem, I. A. T., Gani, A., Mokhtar, S., Ahmed, E., Anuar, N. B., & Vasilakos, A. V. (2016). Big data: From beginning to future. *International Journal of Information Management*, *36*, 1231–1247. https://doi.org/10.1016/j.ijinfomgt.2016.07.009.

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining internet of things security: From CIA to CACA. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/1550147719899374.

Yun, H. (2013). Understanding the use of location-based service applications: Do privacy concerns matter ? *Journal of Electronic Commerce Research*, *14*, 215–230.