https://doi.org/10.48009/1_iis_2021_1-9

# Awareness of mobile device security and data privacy tools

**Loreen M. Powell,** *Bloomsburg University of Pennsylvania, lpowell@bloomu.edu*
**Jessica Swartz,** *University of the Cumberlands, jessica.schwartz@ucumberlands.edu*
**Michalina Hendon,** *University of the Cumberlands, michalina.hendon@ucumberlands.edu*

## Abstract

Today, during the COVID-19 pandemic, the use of mobile devices has become a global norm for society. People use mobile devices for social media applications, internet browsing, banking, e-pay, photography, music, e-mails, directions, timers, applications, work, and education. However, not all mobile devices are properly protected. Thus, it is critical to educate users about mobile device security and data privacy because the consequences of losing personal or organizational data are significant and very challenging to recover. This research explores the literature and details current mobile device security and data privacy issues, terminology, and defensive techniques. Additionally, this research utilized the Delphi approach to form a comprehensive, ranked matrix of well-established mobile security applications.

**Keywords:** Mobile security, data privacy, malware, location traction, remote wipe, mobile security tools

## Introduction

In 2016 there were more than 7.7 billion mobile device users/connections (GSMA Intelligence, 2016). Among those mobile connections, more than 3.7 billion are from smartphone users (Koyuncu & Pusatli, 2019). Baillette, Barlette, and Leclercq-Vandelannoitte (2018) reported that the purchasing of mobile devices surpassed the current sale of the personal computer (PC). The increasing usage of smartphones/mobile internet users has shifted the way in which people interact, access, and store data (Kemp, 2016). For example, mobile devices' connectivity to the internet has allowed users to download games, send e-mails, browse websites, conduct online banking, buy merchandise, access company networks, share data, access social networks, and so much more (Baillette, et al., 2018; GSMA Intelligence 2020).

Furthermore, the recent worldwide COVID-19 pandemic has majority of the world working remotely from home as a mode for practicing social distancing (Stewart & Menon, 2020). Prior to the pandemic, approximately 17 million jobs were directly supported via the mobile ecosystem (GSMA Intelligence, 2016). The Global Mobile Trends 2021 Report predicts that mobile internet usage may increase more from the COVID-19 pandemic (GSMA Intelligence, 2020). The increase of mobile internet users brings about many data privacy and security concerns (Kemp, 2016; Markelj & Bernik, 2015; Rota, Pinchot, & Paullet, 2010; GSMA Intelligence, 2020).

Existing mobile security research has typically focused on passwords (Yazji, Scheuermann, Dick, Trajcevski, & Jin, 2014), voice recognition (Moon, Leung, & Pun, 2003), and finger prints in the authentication stage. While this type of research is valuable, it doesn't adequately protect mobile (GSMA Intelligence, 2016 & 2020). The goal of this paper is to explore, comparre, and rank tools available for individuals to increase digital privacy and security on mobile devices. This paper provides a significant impact upon previous literature and mobile internet users so that they may make better-informed decisions regarding securing and privacy on their mobile devices. The remaining structure of this paper is as follows: brief review of the literature, research purpose, methodology, results, and conclusion.

## Literature review

Today, mobile internet usage is very common. However, the problems and issues surrounding the mobile internet usage include information tracking, leaked, collected, and shared (Koohang, Paliszkiewicz, Nord, Paullet, & Underwood, 2019). Many small businesses or low profile organizational websites otherwise known as "just plain sites" (JPS) place mobile users at risk. For example, JPS may collect unnecessary private information (Aleyasen, Starov, Phung Au, Schiffman, & Shrager. 2015) or may not update email templates to protect account passwords (Bologa, Lupu, Boja, & Georgescu, 2017). Differences between the desktop and mobile versions of websites in terms of security characteristics can lead to abuse going undetected or the introduction of additional vulnerabilities.

Data privacy and security is a current issue in education as more educators are using technology within the classroom (Jamil, Jamil, & Shahzadi, 2019). As digital natives of technology, college students are in the middle of a new enhanced security paradigm shift. Additionally, teens and tweens are also heavily immersed in technology (Koyuncu & Pusatli, 2019). According to Common Sense Media (2015), device ownership among individuals, 8 to 18-years of age, increased from 67% in 2015, to 84% in 2019. Anderson and Jiang (2018) found within United States (US) teens in 2018, only 88% have access to a home laptop and or desktop, however, 95% of teens own a smartphone. These statistics are radically different from 10 years ago. As a result of this rapid increase in usage, many of mobile users may not be educated regarding the importance of mobile privacy and security (Bullen & Morgan, 2016; Anderson & Jiang, 2018).

Moreover, many mobile users are broadening their social media circles, shopping for necessities, and handling personal finances online daily (Ko & Jeng, 2015). The threat of identity theft and downloading malicious spyware/adware is frequent. In 2019 the Pew Research Center (PEW) found that 70% individuals lack confidence in the security of their data online. Meanwhile, 63% of Americans say they lack understanding and/or education in the protection of their information by organizations (Anderson & Jiang, 2018). Users checking their privacy settings and ensuring that their devices are not broadcasting their location is a small question of security that users should reflect upon often.

Koohang et al. (2019) surveyed 184 employees regarding the success variables that may influence users' security and data protection awareness of mobile devices. They concluded that education and awareness of mobile security, privacy, and risks are important. In 2014 the National Science Foundation (NSF) and National Security Agency (NSA) established the GenCyber program. The purpose of GenCyber is to raise awareness regarding mobile security among middle and high school students (Payne, Abegaz & Antonia, 2016; Jiang, Tian, & He, 2017; Smith & Ali, 2019). While this program has been helpful to teens within middle and high school, there is no follow-up awareness programs after high school. Thus, if an employer or university doesn't offer mobile security training, little mobile security awareness is gained after high school. Therefore, there is a need for awareness of mobile security tools after high school.

Furthermore, Pinchot and Paullet (2015) conducted an extensive study of mobile data privacy preventative measures among 187 university students and alumni within a Mid Atlantic university within the US. They found that participants were not as aware of many security and privacy features or tools. Pinchot and Paullet concluded that there is a need for an awareness and education regarding tools available for users to secure their mobile devices and data.

## Securing and Privacy Awareness & Trends

### *Malware*

Malware is an intrusive and disruptive program intended to operate on a device without the owner's knowledge or permission. Often, adware, spyware, key loggers and viruses are also referred to as malware (Karim, Shah, Salleh, Arif, & Noor, 2015).

Futuresight (2011) studied mobile users concerns within 219 countries. This study revealed that an overwhelming 92% of mobile users expressed concern regarding malware applications. Today, many mobile users expect their mobile device to be protected or secured upon purchase. However, mobile devices do not come fully secured with a malware protection app. More alarming, many mobile users do not understand that their device is vulnerable to malware and malicious attacks.

Bruno, Graziano, Balzarotti, and Francillon (2014) reported that malware on mobile devices is an important and evolving issue because there is no coding involved infecting Android applications with malicious programs. Therefore, Android platforms and applications are currently most at risk for malware attacks. As such, many hackers have taken advantage of Android platforms and application vulnerabilities to gain unauthorized access in sending e-mails, accessing unauthorized files and photos, and locking user data. Hence, mobile device users need to be prepared for the increasing number of malware and malicious attacks to come.

Karim et al. (2015) and Lemos, Daniel, and Benatallah (2016) argued that many cyber criminals are beginning to exploit the vulnerabilities of mobile devices. For example, a simple malware and malicious application scan on 20 million apps within a worldwide app store found 52% of the apps to be harmful.

### *Location Tracking*

Tracking mobile devices' location without the user finding out is becoming a common occurrence today. There are undetectable spy applications for mobile devices with location tracking which makes mobile device tracking easier than ever. Whatever the reason is for tracking another person's phone, it is essential for users to understand how to avoid being tracked.

Currently, the establishment and use of maps with voluntary participation of tracking of COVID-19 established through Facebook and researchers from different medical institutions and universities are used to assist on the federal, state, and local levels to disseminate the information that is collected. A partnership formed between Facebook and Carnegie Mellon initiated the Delphi COVID-19 Response Team. Facebook allowed the use of their platform for Carnegie Mellon to solicited data through surveys. The surverys reach and collect information from individuals affected by the various and their symptoms (Wilson, 2020). As organizations are using technology to provide the information voluntarily, the question of where the data will remain after the study can be questioned by the participants.

The US also has Health Insurance Portability and Accountability Act (HIPAA) in place to protect citizen's health information. However, in order to relay information quickly around the world, HIPAA may not always be properly followed during a pandemic. For example, In Singapore a tracking app called TraceTogether is used for monitoring COVID spread. TraceTogether tracks and logs the user's location and meeting with other users through Bluetooth technology. This information is used to report to Singapore's Ministry of Health, the individuals are notified through the app when there is a user that has symptoms. However, regarding the US, they found TraceTogether usage may not be as acceptable as there is no guarantee of privacy protection (Cho, Ippolito, & Yo, 2020). Additionally, Messai & Seba (2020) compared COVID-19 tracing apps regarding privacy and security threats. They found that TraceTogether's malicious developer is open sourse. Thus, the acceptance, use, and privacy of the information along with future implications are all questions that will be discussed in the coming months as privacy compromises are discovered.

### *Data Privacy*

Undoubtedly, privacy is a huge concern for many mobile users as users' data have been stolen and exploited (Alqahtani & Li, 2017). There are many research studies focusing on how to overcome mobile privacy issues. It is important to note that privacy protection includes detecting applications suspected of stealing data or unintended exposure of photos or other data. Data privacy is often associated with privacy browsing mode, privacy browsing, safe browsing, secure app advisor, privacy protection, and wifi security (Yao, Chuang, & Hsu, 2018).

Privacy browsing or incognito mode allows mobile users browse the web without collecting browsing history, cookies, or temporary files. (Zhao & Liu, 2015). Recently, Wu, Gupta, Wei, Acar, Fahl, and Blase (2018) examined 460 participants' perceptions regarding private browsing mode. They found that many users have misconceptions regarding private browsing mode. Thus, agreeing with research by Solove (2005) that privacy is misleading.

Many users confuse privacy browsing mode with safe browsing features provided by security applications. Safe browsing or phishing blacklist includes blocking malicious links and phishing websites. Three of the widely used safe browsing blacklist are Google Safe Browsing (GSB), PhishTank (PT), and OpenPhish (OP) (Bell & Komisarczuk, 2020).

Like safe browsing, remote wipe is another essential component needed within a privacy tool. Remote wipe means the app allows data to be erased from a smartphone remotely. Yu, Wang, Sun, Zhu, Gao, and Jing (2014) argue because remote wipe methods typically need WiFi or a SIM card for cellular network connection it is difficult to protect data if a mobile device is stolen. They provided a novel approach to allows users to delete data remotely without WiFi or SIM card available. Similarly, secure app advisor warns the user if apps downloaded on the mobile device are safe.

A study by Yao, Chuang, and Hsu (2018) examined 12 mobile security and antivirus features. A two-dimensional, Kano Model questionnaire was utilized to survey users. Their study found malware prevention, safe browsing, parental control, and privacy protection had the most impact for customer satisfaction. They also found that females tend to consider remote lock and locate and wifi security as important features. Lastly, non-technological users desire garbage file cleanup, remote lock and locate and secure app advisor was found.

Another study by Alqahtani and Li (2017) utilized an PPAndroid-Benchmarker, to analyze privacy functions on an Android device. They applied 165 apps with privacy features to PPAndroid-Benchmaker. They found that PPAndroid-Benchmaker was successful in moving information sources and sinks. As well as, many applications required additional configuration or changes in their default settings to ensure they were fully enabled. However, they did not disclose the mobile security apps in which default settings needed to be changed.

## Purpose of the study

The purpose of this paper is to provide and compare a short list of tools that can be used by mobile users alike to protect their data and increase their personal security in digital tasks. Specifically, this research seeks to provide a short list of well-established mobile security and privacy tools, sort the tools by features, and rank those tools by features, cost value, and platforms.

## Methodology

A review of literature was conducted over a nine-month period to determine the most commonly used mobile security and privacy tools. Specifically, the three authors conducted a content analysis of website reviews and online literature for over 50 mobile security products. Next, using the Delphi approach, the three authors compiled a list top of twenty of the most common and well-established mobile security software tools.

Next, a qualitative web content analysis and app testing were conducted to examine the applications for remote wipe, privacy protection, secure app advisor, and wifi security features. The authors examined the applications features identified as essential within the literature.

Moreover, this research utilized a qualitative web content analysis approach to analyze the presence the platform, cost, and privacy feature concepts of each of the twenty software tools. Data obtained was tabulated and presented in a matrix format.

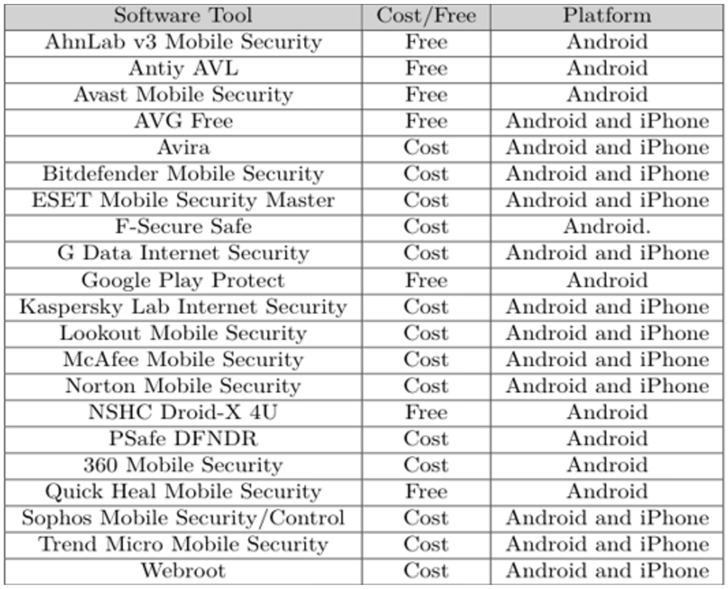
Finally, the Delphi approach was utilized to rank the software tools by features, cost value and platforms. The authors served as the panel of experts. Each author studied IT security as part of their doctoral program and has experience within the industry or with academic research. The authors interacted via e-mail ranking the software tools and sent the information back and forth twelve times until a consensus was reached regarding the rankings.

## Results

### Comprehensive Matrixes Recommendations

The best way to protect a mobile device from malware is to download and install a mobile security application. Malware prevention includes scanning for viruses and malware when applications are downloaded to mobile devices. Table 1 provides a summary of the most common and well-established mobile security applications to help protect against malware and viruses.

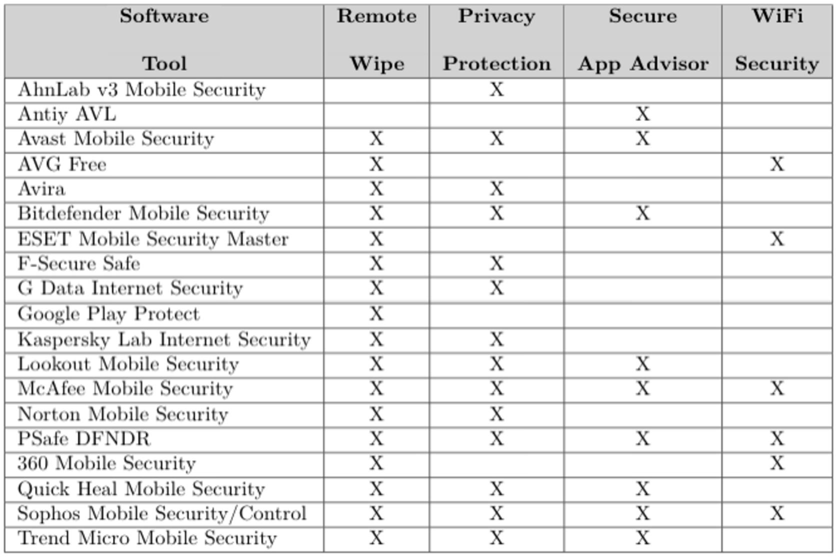
**Table 1.** Matrix of the most common and well-established mobile security applications to help protect against malware and viruses



| Software Tool | Cost/Free | Platform |
|---|---|---|
| AhnLab v3 Mobile Security | Free | Android |
| Antiy AVL | Free | Android |
| Avast Mobile Security | Free | Android |
| AVG Free | Free | Android and iPhone |
| Avira | Cost | Android and iPhone |
| Bitdefender Mobile Security | Cost | Android and iPhone |
| ESET Mobile Security Master | Cost | Android and iPhone |
| F-Secure Safe | Cost | Android. |
| G Data Internet Security | Cost | Android and iPhone |
| Google Play Protect | Free | Android |
| Kaspersky Lab Internet Security | Cost | Android and iPhone |
| Lookout Mobile Security | Cost | Android and iPhone |
| McAfee Mobile Security | Cost | Android and iPhone |
| Norton Mobile Security | Cost | Android and iPhone |
| NSHC Droid-X 4U | Free | Android |
| PSafe DFNDR | Cost | Android |
| 360 Mobile Security | Cost | Android |
| Quick Heal Mobile Security | Free | Android |
| Sophos Mobile Security/Control | Cost | Android and iPhone |
| Trend Micro Mobile Security | Cost | Android and iPhone |
| Webroot | Cost | Android and iPhone |

To protect user privacy, many locking mechanisms enable password-locking/unlocking, wherein typically none or all a mobile device's features are accessible to the user. Since typing a password every time a user picks up the device is tedious, such practices often fail due to non-use. Mobile device users may prioritize convenience over strong security, thereby accidentally sharing sensitive information with unintended audiences. Solutions that address the users' communication privacy, while enabling protection of business content are essential. Therefore, users must consider mobile security applications to help protect their privacy while using their devices over multiple contexts including personal, educational, and business. There are several features that should be considered when choosing the best fit for a mobile security application. Table 2 provides a summary of the most common mobile security applications with remote wipe, privacy protection, secure app advisor, and wifi security.

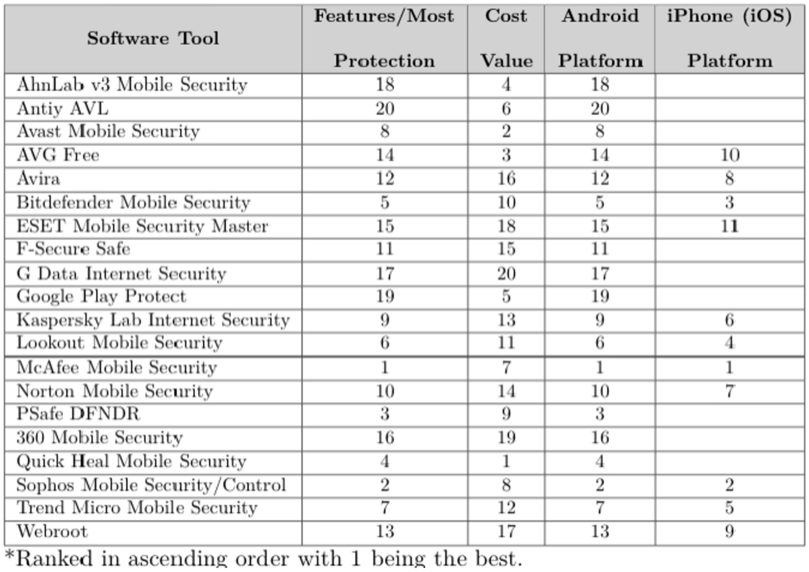
**Table 2.** Most common mobile security applications



| Software | Remote | Privacy | Secure | WiFi |
|---|---|---|---|---|
| Tool | Wipe | Protection | App Advisor | Security |
| AhnLab v3 Mobile Security | | X | | |
| Antiy AVL | | | X | |
| Avast Mobile Security | X | X | X | |
| AVG Free | X | | | X |
| Avira | X | X | | |
| Bitdefender Mobile Security | X | X | X | |
| ESET Mobile Security Master | X | | | X |
| F-Secure Safe | X | X | | |
| G Data Internet Security | X | X | | |
| Google Play Protect | X | | | |
| Kaspersky Lab Internet Security | X | X | | |
| Lookout Mobile Security | X | X | X | |
| McAfee Mobile Security | X | X | X | X |
| Norton Mobile Security | X | X | | |
| PSafe DFNDR | X | X | X | X |
| 360 Mobile Security | X | | | X |
| Quick Heal Mobile Security | X | X | X | |
| Sophos Mobile Security/Control | X | X | X | X |
| Trend Micro Mobile Security | X | X | X | |

Based upon tables 1 and 2, the authors ranked the software tools. Table 3 provides the list of software tools according to features, cost value, and platform.

**Table 3.** Author ranked information matrix to software tools



| Software Tool | Features/Most | Cost | Android | iPhone (iOS) |
|---|---|---|---|---|
| | Protection | Value | Platform | Platform |
| AhnLab v3 Mobile Security | 18 | 4 | 18 | |
| Antiy AVL | 20 | 6 | 20 | |
| Avast Mobile Security | 8 | 2 | 8 | |
| AVG Free | 14 | 3 | 14 | 10 |
| Avira | 12 | 16 | 12 | 8 |
| Bitdefender Mobile Security | 5 | 10 | 5 | 3 |
| ESET Mobile Security Master | 15 | 18 | 15 | 11 |
| F-Secure Safe | 11 | 15 | 11 | |
| G Data Internet Security | 17 | 20 | 17 | |
| Google Play Protect | 19 | 5 | 19 | |
| Kaspersky Lab Internet Security | 9 | 13 | 9 | 6 |
| Lookout Mobile Security | 6 | 11 | 6 | 4 |
| McAfee Mobile Security | 1 | 7 | 1 | 1 |
| Norton Mobile Security | 10 | 14 | 10 | 7 |
| PSafe DFNDR | 3 | 9 | 3 | |
| 360 Mobile Security | 16 | 19 | 16 | |
| Quick Heal Mobile Security | 4 | 1 | 4 | |
| Sophos Mobile Security/Control | 2 | 8 | 2 | 2 |
| Trend Micro Mobile Security | 7 | 12 | 7 | 5 |
| Webroot | 13 | 17 | 13 | 9 |

*Ranked in ascending order with 1 being the best.

## Conclusion

While threats can be contained or mitigated with the use of cybersecurity tools; without proper introduction or education of available tools, the security of the mobile user's daily use can be vulnerable. Existing research has shown that mobile devices are vulnerable to security attacks. Additionally, there is an abundance of information and tools regarding mobile device security which often is confusing for one to know or understand which tool is best suited to secure their mobile device. This paper provided valuable information for users to better understand mobile devices security and tools.

It is important to note that this research is not without limitations. First, this research is limited as it is theoretical in nature because it did not test any of the information described. Second, it is also limited in that it only assumes users do not understand how to protect their mobile devices. It also assumes that mobile devices are not secure. Additional research should address these limitations.

Regardless of the limitations, this paper has practical implications for higher education faculty teaching mobile security as it adds to the existing body of literature. This research is also important because it suggests practical tools for end user's mobile devices to secure and preserve critical data. In addition, it provides examples of tools users can implement to thwart attacks and keep data safe and provides an order rank of tools.

## References

Aleyasen, A., Starov, O., Phung Au, A., Schiffman, A., & Shrager, J. (2015). On the privacy practices of just plain sites. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, ACM, 1– 10.

Alqahtani, S. I & Li, S. (2017). Ppandroid-benchmarker: Bench-marking privacy protection systems on android devices. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ACM, New York, NY, USA 19. 1–10. https://kar.kent.ac.uk/69561/1/ppandroidbenchmarker.pdf

Anderson M. & Jiang, J. (2018). Teens, social media & technology 2018. *Pew Research Center*, 31.

Baillette, P., Barlette, Y. & Leclercq-Vandelannoitte.A. (2018). Bring your own device in organizations: Extending the reversed it adoption logic to security paradoxes for CEOS and end users. *International Journal of Information Management*, *43*, 76–84.

Bell S & Komisarczuk, P. (2020). An analysis of phishing blacklists: Google safe browsing, openphish, and phishtank. In *Proceedings of the Australasian Computer Science Week Multiconference*, 1–11.

Bologa, R., Lupu, A. R., Boja, C. & Georgescu, T. (2017). Sustaining employability: A process for introducing cloud computing, big data, social networks, mobile programming and cybersecurity into academic curricula. *Sustainability*, *9*(12), 2235.

Bruno, L., Graziano, M., Balzarotti, D. & Francillon, A. (2014). Through the looking-glass, and what eve found there. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, San Diego, CA, USENIX Association.

Bullen, M. & Morgan, T. (2016). Digital learners not digital natives. *La Cuestión Universitaria*, *7*, 60–68.

Cho, H., Ippolito, D. & Yu, Y.W. (2020). Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511*.

FutureSight. (2011). User perspectives on mobile privacy. GSMA Intelligence, Group Special Mobile Association (GSMA) http://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011

GSMA Intelligence (2016). Global mobile trends.

GSMA Intelligence (2020) Global mobile trends: Navigating COVID-19 and beyond. https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=58621970&file=141220-Global-Mobile-Trends.pdf

Jamil, J., Jamil, S. & Shahzadi, U. (2019). Computer ethics: Perspectives of contemporary teachers. *Pakistan Journal of Social Sciences (PJSS)*, 39(1), 295 – 304.

Jiang, P., Tian, X., Xin, C., & He, W. (2017, June). Teaching Hands-On Cyber Defense Labs to Middle School and High School Students: Our Experience from GenCyber Camps. In *Proceedings of EdMedia+ Innovate Learning* Conference. Association for the Advancement of Computing in Education (AACE), 640-644.

Karim, A., Shah, S. A. A., Salleh, R. B., Arif, M. & Noor, R. M. (2015). Mobile botnet attacks–an emerging threat: Classification, review and open issues. *KSII Transactions on Internet and Information Systems (TIIS)*, *9*(4), 1471–1492.

Kemp, S. (2016). Digital in 2016. https://wearesocial.com/special- reports/digital-in-2016.

Ko, Ch. H., & Jeng S. (2015). Mobile technology adopted in hotel sales. *The International Journal of Organizational Innovation*, *8*(2), 172-183.

Koohang, A., Paliszkiewicz, J., Nord, J. H., Paullet, K. & Underwood, T. (2019). Predictors of success in security and data protection awareness of mobile devices: trust and privacy, *Issues in Information Systems*, *20*(1), 1-11.

Koyuncu, M. & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*.

Lemos, A. L., Daniel, F. & Benatallah, B. (2016). Web service composition: a survey of techniques and tools. *ACM Computing Surveys (CSUR)*, *48*(3), 33.

Markelj B. & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, *20*(1), 84–89.

Messai, M., L. & Seba, H. (2020). Short paper: Privacy comparison of contact tracing mobile applications for COVID-19. https://arxiv.org/pdf/2010.03232.pdf

Moon, Y. S., Leung, C. C. & Pun, K. H. (2003). Fixed-point GMM-based speaker verification over mobile embedded system. In *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, WBMA '03, 53–57.

Payne, B. R., Abegaz, T., & Antonia, K. (2016). Planning and Implementing a Successful NSA-NSF GenCyber Summer Cyber Academy. *Journal of Cybersecurity Education, Research and Practice*, *2*(3).

Pinchot, J. & Paullet, K. (2015) Use of preventative measures to protect data privacy on mobile devices. *Journal of Information Systems Applied Research*, *8*(2) 44-51.

Rota, D., Pinchot, J. & Paullet, K. (2010). How mobile technology is changing our culture. In: *The Proceedings of CONISAR 2010*, 39–48.

Smith, D., T. & Ali, A. I., (2019) You've been hacked: a technique for raising cyber security awareness. *Issues in Information Systems*, *20*(1), 186-194.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154, 477.

Stewart, K. & Memon A. (2020). *COVID-19 pandemic: How to navigate the transition to remote work.* https://www.weforum.org/agenda/2020/03/covid-19-transition-to-remote-work/

Wilson, M. Y. (2020). *Facebook & Carnegie Mellon University COVID-19 symptom map.* https://betanews.com/2020/04/20/facebook-carnegie-mellon-university-covid-19-symptom-map/

Yao, M. L., Chuang, M. C., & Hsu, C. C. (2018). The kano model analysis of features for mobile security applications. *Computers & Security*, *78*, 336–346.

Yazji, S., Scheuermann, S. Dick, R. P., Trajcevski, G. & Jin, R. (2014). Efficient location aware intrusion detection to protect mobile devices. *Personal and Ubiquitous Computing*, *18*(1), 143–162.

Yu, X., Wang, Z., Sun, K., Zhu, W. T., Gao, N. & Jing, J. (2014). Remotely wiping sensitive data on stolen smartphones. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, 7–542.

Wu, X., Gupta, P., Wei, M., Acar, Y., Fahl, A. & Ur, B. (2018). Your secrets are safe: How browsers' explanations impact mis- conceptions about private browsing mode. In *Proceedings of the 2018 World Wide Web Conference*, 217–226.

Zhao B & Liu, P. (2015). Private browsing mode not really that private: Dealing with privacy breach caused by browser extensions. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, IEEE, 184–195.