Mobile App Data Aggregation: Security and Privacy Implications for Consumers

Hannah R. Marriott (✉), Benjamin G. Sanders and Anna M. Penrose

Business School, University of Winchester, Hampshire, UK
{Hannah.Marriott, Ben.Sanders, Anna.Penrose}@winchester.ac.uk

Abstract. Global usage of mobile devices and their services is at all all-time high with millions of application (app) downloads occurring daily. Although mobile apps are inherently useful and easy to use, negative personal experiences and negative press surrounding the protection of consumers' personal information has led to significant concerns surrounding data privacy and security. This working paper critically reviews consumers' perceptions of mobile app privacy and security, and the impact of such on their mobile app adoption intention, whilst considering how the new General Data Protection Regulation (GDPR) initiative aims to enhance data protection. Discussions of surrounding literature subsequently outlines scopes for further insight in this area.

Keywords: Mobile, security, privacy, GDPR, consumer behaviour, data aggregation

1 Introduction

Although modern mobile devices provide a number of advantages from a wide range of communication technologies and storing a plethora of information, they can also pose a number of privacy and security concerns. Given their ubiquity, increasing functionalities, and decreasing related acquisition and operating costs, it is not surprising that mobile phones have been embraced in a variety of ways to aid data collection efforts around the world.

It is widely acknowledged that markets have been reinvented from the traditional price-based approach to a data rich economy with more comprehensive information about human wants and needs. These data rich markets covertly capture consumer preferences, behaviours and personal information and, juxtaposed with sophisticated matching algorithms, capitalise on the power of data to maximise profit. As users readily engage with a greater range of mobile apps, there is a corresponding need to raise awareness of the surveillance economy.

2 Consumers' perceptions of privacy

2.1 The privacy paradox

The dichotomy between a person's attitude towards information privacy and their actual behaviour, despite such concerns, is referred to as the "privacy paradox". In this modern age, individuals divulge extensive amounts of personal information daily; from browsing websites to posting on social networking sites. Modern consumers are aware of website "cookies", data storing, the longitudinal nature of electronically shared information, and the potential for data hacking and identity theft, yet their online habits are not representative of such concerns. This has raised further awareness to the existing "attitude-behaviour" gap and has prompted questions whether the privacy paradox exists within this modern digital age [e.g. 18]. As such, literature recognises that consumers undergo a "risk-benefit" evaluation within this gap, which are deemed to be none or negligible based on a rational or irrational decision-making process [e.g. 3].

The privacy paradox has more recently been acknowledged to occur at the retailer level. Ginosar and Ariel [9] observe that retailers are equally concerned with the handling of their consumers' personal information, but nevertheless see the importance in obtaining, storing and using that information for the benefit of their websites; the authors refer to this as the "website privacy paradox". Although this is an interesting finding, as the amount of literature examining organisational behaviour in conjunction with consumer attitudes is significantly underdeveloped, this proposed extension of the privacy paradox can be argued to be more closely related to security, as security relates to how secure the collected information is kept once obtained. This continues the theme in online retailing literature that a cross over between privacy and security concerns still exists [19].

2.2 Privacy in the digital age

The Internet has provided its users with a plethora of services for a variety of industry and consumer needs and has revolutionised the online retailing environment. However, with increased functionality and opportunities comes inherent dangers. Despite the rapid development of online services, concerns relating to personal data privacy remains prevalent among modern consumers. The essence of privacy is how much control users have, or perceive themselves to have, over their personal information [25]. The level of control over the information greatly affects consumers/users privacy perceptions and their subsequent information disclosure [11; 26], security perceptions (Johnson et al., 2018; 23] and overall technology or service adoption intentions [e.g. 7].

Vast amounts of privacy-related literature has been published focusing on the Internet and websites in general (e.g. 2) however, increased attention has been given to electronic commerce (e-commerce), mobile commerce (m-commerce), social networking sites (SNS), location-based services, mobile cloud computing, and mobile applications (apps). The consensus across research areas is that users who are concerned for their personal information privacy are more likely to utilise protective measures (7], provide inaccurate or incomplete information [21; 23], or rely more heavily on vendor reputation [7]. Research has recognised that more examination into the affects of risks to information privacy towards consumers' motivations to continue sharing their personal information within the mobile realm [7].

2.3 Mobile app privacy

Although most online privacy-related literature concerns consumers' privacy perceptions towards websites, more recent literature has recognised additional privacy concerns within the mobile environment, particularly in relation to mobile applications. Pentina et al. [22] found that millennial mobile app download intention was negatively affected by privacy concerns but positively affected by their information and social needs, and thus confirmed that the privacy paradox remains prominent within the mobile app realm. Wottrich, Reijmersdal and Smit [26] further established that app value, being the benefits of downloading and using it, outweigh the "costs", being intrusiveness and privacy concerns, and confirmed the notion of a privacy trade-off. Gu et al. [10] considered consumers' intention to download an app from the Android app store and found that permission sensitivity positively contributed to overall privacy concerns, which negatively effects their download intention. However, permission justification and app popularity had negative effects on privacy concerns and overall download intention, suggesting that privacy goes beyond the traditional privacy paradox and is instead affected by trust. Research recommends future research be invested in the role of security perceptions [22], more contextual understanding [10; 26], differences between paid and free apps [26], the influence of electronic word-of-mouth [10], and the influence of personality and cultural variables [22].

Despite privacy assurances of a plethora of mobile app vendors, evidence suggests that users are unaware of the potential threats to personal privacy posed by third party add-on apps. At the time of writing, 50 million Facebook users had their data exposed through using a quiz app built by Cambridge Analytica. Moreover, thousands of app developers including Tinder and FarmVille mine vast quantities of data about users and their online friends, through Facebook's overly permission 'Graph Application Programming Interface' (API); the interface through which third parties interact with Facebook's platform.

3 Consumers' awareness of mobile security features

3.1 Security in the digital age

The concept of privacy is concerned with the level of control that users have over their personal information. However, security, relates to the level of action a vendor takes to ensure the technology being used is secure (Johnson et al., 2018); creating a balance between privacy and security concerns is essential for behavioural adoption intention. As with privacy, most consumer-based security-related literature surrounds the Internet or websites, SNS and e-commerce. However, most research considers security alongside privacy concerns, rather than examining security independently. For example, McCole et al. [20] and Shukla [24]) consider the two main types of uncertainty in online buying to be system dependent, being the security concern, and transaction-specific, being the privacy concerns. This is further demonstrated by Arpaci et al. [1] who found that security and privacy have a significant collaborative effect on attitudes towards cloud services. As such, it can be argued that to further understand consumers' security concerns towards mobile apps, understanding into their perceived control, once their information has been obtained by vendors, must be considered in future research. Furthermore, due to the lack of understanding into consumers' mobile app security perceptions, the scope for further research in this sphere is extensive.

3.2 Mobile app security

Downloading mobile applications entails consumers "giving away" their data to the app publisher. Although this is done at their own free will, some questions have arisen if consumers are aware or have distorted perceptions of apps and their subsequent risk perceptions of them [4]. Literature reveals a variety of consumer behaviours across research settings. Buck et al. [4] explains that security and privacy concerns have minor relevance in such situations. In examining mobile device users' security perceptions, Imgraben et al. [16] found that users generally do not understand the risks surrounding cyber criminals' ability to take and sell their collective identities, with most not perceiving cybercrime to be a real threat. However, Hubert et al. [12] found that, in the case of mobile shopping, security concerns have the potential to increase as the awareness of control is higher in location sensitive apps.

As with privacy, a security paradox also seems to exist, subject to varying degrees across contexts; as such "selective perception" [4] or trade-off behaviours appear to be prominent amongst consumers. Accordingly, further attention should be drawn to the privacy and security paradoxes and their relationships between them to gain deeper insight into the factors negatively affecting consumers' mobile app purchases and usage.

4 Legal Regulation of Mobile App Data

4.1 The GDPR

The General Data Protection Regulation (GDPR), introduced in May 2018, is the current focus for many organisations as it governs any business doing business with a person in Europe. It is seen by many as a long overdue improvement to the current legislation which has not kept pace with changing technology, data use and consumer need of control over personal data. As such, the UK will be adopting GDPR and superseding the 1998 Data Protection Act (DPA) with the Data Protection Bill on 25th May 2018. The GDPR address the need to protect the Personally Identifiable Information (PII) and the Sensitive Personal Data (SPD) that they hold.

The GDPR [8] defines PII as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". Sensitive Personal Data (SPD) is handled slightly different and is considered "*special categories of personal data*" (listed in Article 9) and include genetic data, and biometric data where processed to uniquely identify an individual' [13]. Accordingly, the GDPR is designed to place more control back into the hands of consumers; to be better informed about how their data is used and have more choice on what and how their data is shared. Principally, they will have more power to demand access and modification to their held data; a right to be forgotten and raise a complaint.

Article 5 outlines the data protection principles and business obligations in which personal data shall: (1) be processed lawfully, fairly and in a transparent manner, (2) be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes, (3) be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, (4) be accurate and, where necessary, kept up to date, (5) be kept in a form which permits identification of data subjects for no longer than is necessary, (6) be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, and (7) be the responsibility of the controller to be able to demonstrate compliance with the GDPR [14].

Under *Lawfulness and Transparency* (Article 5; 14), privacy notices and 'opt ins' can no longer be implicit with a download or a tick box where information relating to what a business may do with PII be hidden within pages of terms and conditions. Transparency means that an organisation needs to be open and honest with how, where and with whom it processes and shares data, which must be explained before any sign up. It also needs to be written in plain English. For children under the age of 13, the rules are significantly more strict; it will be interesting to see how apps respond to the copywriting challenge ahead (i.e. how do you explain profiling to an eight year old downloading a game?). It must also be noted that apps that sell data to third parties will not be stopped from doing so, but will need to comply.

Article 25, concerning 'data protection by design and by default', has significant press coverage due to the impact on businesses; particularly those who have not already build such an ethos into their existing operations. As consumers become more aware of their rights, mobile applications will need to change the way they operate to ensure visible compliance.

4.2 Legal protection and regulation

Article 6 outlines the lawful basis for processing [15] and, while contract or legal obligation are reasonably easy to understand and justify, the basis of consent and legitimate interest are more challenging and the last year has seen much debate around these two bases in the marketing world [6]. Although some apps will operate under contract or legitimate interest, many will need to gain consent for the processing they perform. It is therefore important that the lawful basis and purpose are thoroughly considered in advance, along with the wording for a privacy notice.

5 Challenges and Opportunities for App Developers

The GDPR presents significant challenges for application developers. There is a significant task for app owners to undergo a 're-permissioning' exercise for data subjects already using apps that have not signed up to use the principles of GDPR. This creates a certain anxiety for many organisations who fear inaction or opt-out as a result of the necessary action. Furthermore, in the future, if a company wants to change the purpose for which the data is collected, all data subjects will need to provide informed consent.

Consumers seldom understand the level of PII needed for an application to work effectively, or to provide the best customer experience, nor do they want to read extended privacy notices on a mobile device. Consumers do, however, have an expectation of convenience. Building in GPDR compliance while maintaining speed and convenience will take time and skill. App owners will also need to consider how to automate access and modification to PII for data subjects. Under GDPR this access must be granted within 30 days and be at no cost to the subject. Without automation, this could create significant overhead to the organisation and frustration or lack of trust with the data subjects.

Securing information held on laptops and other mobile devices (commonly known as 'unstructured data') will also be a challenge as it is often more difficult to track and is at a greater risk of being compromised because it is not behind the company firewall. Thus, two factor authentications and encryption are likely to become commonplace in any application collecting personal data. If a data breach does occur, companies must report it to the ICO (or relevant body in their country) and all affected data subjects within 72 hours of a breach occurring. For mobile applications this means a greater emphasis on data security, which will be a significant challenge. Consumers will see much more publicity around data breaches, and as we've seen from the recent Cambridge Analytica press report, the reputational impact could be significant [5]. Accordingly, businesses must take action in response to GDPR or risk hefty fines (4% annual turnover or £20 million, whichever is more). There is also an opportunity; if apps organise and keep accurate, safe, and accessible data, not only will they benefit from a more efficient system and 'smart' (opposed to 'big') data, they will also benefit from increased trust and client loyalty [17].

6 Conclusions

Despite the "smart" nature of mobile devices and their apps, consumer perceptions and organisational protection surrounding the storage and use of personal data remains a contemporary issue for practitioner and theorist insight. From the consumer perspective, a paradox surrounding privacy and security concerns remain evident with little understanding into why this paradox still exists in this modern digital age. Furthermore, with the introduction of the GDPR, practitioners must now be more mindful and proactive with the protection of collected consumer data. This research has drawn attention to the need to consider both the

consumers' and practitioners' security and privacy perspectives in future research and proposes consideration begin with the privacy and security paradox alongside the introduction of the new GDPR regulations.

References

1. Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, *45*(1), 93-98.
2. Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.
3. Barth, S., & de Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058.
4. Buck, C., Horbel, C., & Kessler, T. (2017). *A four-factor framework of consumers' perception of mobile applications in context* (No. 64). Bayreuther Arbeitspapiere zur Wirtschaftsinformatik.
5. Cox, J. (21 March, 2018). Facebook stock drops even further in the wake of Cambridge Analytica scandal. *Independent*. Accessed on https://www.independent.co.uk/news/business/news/facebook-share-price-cambridge-analytica-trump-data-breach-twitter-social-media-a8266701.html
6. DMA. (Aug, 2017). GDPR Consent or legitimate interest? *DMA*. Accessed on https://dma.org.uk/article/gdpr-consent-or-legitimate-interest-email-marketers-need-both
7. Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*(1), 214-220.
8. GDPR. (2018). Article 4 Definitions. *General Data Protection Regulation.* Accessed on https://gdpr-info.eu/art-4-gdpr/
9. Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing?. *Information & Management*, *54*(7), 948-957.
10. Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*(1), 19-28.
11. Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111-123.
12. Hubert, M., Blut, M., Brock, C., Backhaus, C., & Eberhardt, T. (2017). Acceptance of Smartphone-Based Mobile Shopping: Mobile Benefits, Customer Characteristics, Perceived Risks, and the Impact of Application Context. *Psychology & Marketing*, *34*(2), 175-194.
13. ICO. (2018a). Key Definitions. *Information Commissioner's Office*. Accessed on https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/
14. ICO (2018b). Principles. *Information Commissioner's Office*. Accessed on https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/
15. ICO. (2018c). Lawful basis for processing. *Information Commissioner's Office*. Accessed on https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

16. Imgraben, J., Engelbrecht, A., & Choo, K. K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347-1360.
17. Ismail, N. (11 Jan, 2018). How will GDPR improve the customer experience for consumers? *Information Age*. Accessed Age. Accessed on http://www.information-age.com/will-gdpr-improve-customer-experience-consumers-123470312/
18. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*(1), 122-134.
19. Marriott, H. R., Williams, M. D., & Dwivedi, Y. K. (2017). Risk, privacy and security concerns in digital retail. *The Marketing Review*, *17*(3), 337-365.
20. McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, *63*(9-10), 1018-1024.
21. Paine, C., Reips, U.D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.
22. Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*(1), 409-419.
23. Roca, C. J., García, J. J. & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.
24. Shukla, P. (2014). The impact of organizational efforts on consumer concerns in an online context. *Information & Management*, *51*(1), 113-119.
25. Westin, A. F. (1967). Privacy and freedom. *New York: Atheneum*.
26. Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2017). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*(1), 44-52.