“Why Sideload?” User Behaviours, Interactions and Accessibility Issues Around Mobile App Installation

Craig Goodwin
Keele University, Staffordshire, UK
c.goodwin@keele.ac.uk

With the increase of smartphone ownership year by year, the accessibility of mobile application increases too. Application sideloading is a behaviour identified as the act of installing applications through unofficial means. Moreover, sideloading as a study is insufficiently researched in relation to its occurrence in smartphone usage. This position paper describes sideloading behaviour in context to accessibility, interaction, security, problematic smartphone uses and its occurrences in other devices. The research aims to identify those who sideload, the causes of sideloading and the behavioural differences dependent on the device used with a future intention of reviving and highlighting this field of research.

HCI, Smartphones, Android, iOS, Sideloading, Applications

1. INTRODUCTION

The research presented in this position paper proposes and focuses on the causal effect of mobile application accessibility and installation regarding sideloading on both Android and iOS operating systems. As of March 2019, Android and iOS dominate the mobile operating system market share with Android at 75% and iOS at 22% (StatCounter Global Stats, 2019). Roughly 2.5 billion people own a smartphone with internet connectivity and this figure is rising steadily year by year (Pewglobal, 2019).

Since Android and iOS have different ideologies regarding the open and closed source nature of their operating systems, the varied nature of application sideloading is apparent. With this in mind, we can establish a hypothesis that sideloading has multiple causes in reference to the relationship between access and installation. The act of sideloading requires an alteration in what would be considered official access and/or installation.

2. BACKGROUND & RATIONAL

The rational for researching the topic of sideloading and specifically the user behaviours, attitudes and accessibility issues is valid as there is a lack of research in this research area. (Bretniger, Tully-Doyle & Hassenfeldt, 2019). Due to the timely nature of user behaviour research, the evolution of smartphone technology and the varied and changing demographics of smartphone users, it is important that we research this area in depth with longevity. Whilst mobile security is an active area of research certain areas such as sideloading in relation to consumer habits, human psychology and interaction behaviour are neglected in the academic literature. On the other hand, there is further direction to restart research into Third Party Marketplaces which is often where applications involved in sideloading are found.

The etymology of sideloading (and its behaviours) in relation to smartphones can be historically described as the act of installing an application through unofficial means following the language pattern of download and upload (Branwyn, 2000). This can be achieved in many ways, but its cause is typically understood to be that of circumventing an official means of installing an application. This can often be done out of necessity due to the unavailability of applications on official marketplaces such as the Google Play store and iOS App Store (whether nefarious applications or not).

Progressive Web Applications (PWAs) are, technically, semi-sideloaded applications, they are not widely adopted as an industry standard (Khan et al., 2019) due to the difficulty in adapting the

technology in certain applications (such as gaming), therefore whilst novel discussion can be gained and will be discussed in the literature, it is not an area with a research direction applicable to this PhD.

Activist communities which purposely circumvent official application installation on official marketplaces due to anti-corporate and anti-capitalist agenda are difficult to locate and converse with. This is due to many choosing to stay anonymous online due to potential legal issues, though this form of activism is valid to suggest as a cause of sideloading (Kirillov 2020).

Problematic smartphone use as a term, potential disorder and behavioural issue is widely studied in the psychological literature. Its relation to sideloading behaviour would be difficult to determine but it could be hypothesised that they are related.

3. RESEARCH IN CONTEXT

Historical instances of application sideloading gives us insight with significant case studies with mention to sideloading. The context of these past events highlights key justifications for researching this area.

In mid-2016, Pokémon Go (an AR mobile game) was announced with fragmented release dates worldwide due to the server demands expected. Pokémon is an extremely popular worldwide media franchise, expanding into anime, video and trading card games with an expansive audience in popular culture with iconic semiotics. For example, in 2016, South Korean players travelled in huge numbers to a remote part of the border with North Korea to circumvent restrictions on geo-mapping in the country (Gibbs, 2016). Due to the hysteria and cultural significance of the game, many users elected to sideload the application before release date. A small proportion of those who sideloaded the application were misdirected to the wrong files, or worse, an infected version. This behaviour, where the "fear of missing out" blinds the smartphone user in applying enough security protocols is of great interest.

Similarly, in 2018 the popular video game Fortnite was released outside of the Google Play Store to avoid paying 30% cut on application transactions (Brady, 2018). This highlighted that developers are not fixed to releasing applications on official marketplaces. Furthermore, consumers were and will always be at risk for sideloading applications due to the lack of security awareness. If developers continue to release their applications outside of official marketplaces, we can postulate and theorise a future event of significant calibre with the potential for similar negative consequences.

With consumers in 2020 having an average of 6.58 IoT devices per person (Statista, 2016), it is important that security measures are in place to prevent naïve behaviours from being compromised. This concern is further alarming when we consider that the average age for the adoption of the first smartphone is now 10.3 years old (Influence Central, 2016) and that over 50% of 10-year olds own a smartphone (Ofcom, 2018). The prevention of sideloading is not acceptable should the smartphone user be attentive and educated about the advantages and disadvantages.

Sideloading is currently the only method to install Google Applications on Huawei devices purchased after May 19th, 2019. The BBC (2020) reported on the implications and security risks of sideloading Google's applications due to the inability to confirm the authenticity of the application source. Moreover, the procedures that the consumer must consider when now installing these applications heighten the security.

4. METHODS

This research will apply causal methodologies using focus groups, quantitative surveys and quasi experimental studies.

The first study intends to explore attitudes towards sideloading. This will be conducted via focus groups with the aim of elaborating on discourse with a cohort of participants who will hopefully highlight significant and noteworthy attitudes towards sideloading and will be grounding for the creation of a large-scale survey.

Secondly, we aim to understand the initial opinions and attitudes of sideloading from the focus group which can then be formulated and constructed into the questions for the survey. Quantitative research in this context is the obtaining of data through targeted surveys on the online thread boards of Reddit and posted collectively on social media websites. These surveys will be administered to participants who are actively sideloading on both android and iOS devices. The purpose of this is to understand the causality of this activity and to distinguish whether participants are aware of the implications involved.

The third part of the research will use quasi-experimental methodologies and explore user interactions when controlling a mobile device. In this experiment, we want to premeditate a cause in order to observe its effect. In this instance, we will be developing and changing certain features of an application on a customised version of Android and iOS and setting participants with tasks to complete. The phone will also have a screen capture and touch-tracking application hidden and running whilst the experiment is being conducted to analyse

the user decision process. The aim will be to provide insights into how far users will go to complete tasks in reference to usage of third-party marketplaces, privacy concerns or lack thereof and how responsive to permission presented when installing applications.

Case studies as those mentioned in Section 3 can also be explored in depth as they provide historical context to many of the behaviours seen in smartphone use.

There is also scope for research in areas aside from smartphones. Sideloading occurs in other devices and has clear significance in legal areas such as the right to repair movement. Sideloading research is not limited in device, therefore the behaviours and attitudes are ubiquitous in nature.

5. SUMMARY

In summary, this project aims to answer the question: **Why sideload?** But more specifically:

- ***"What are the behaviours, interactions and attitudes surrounding unofficial mobile application installation"?***
- ***"How do consumers use and interact with methods of sideloading and can this cause wider issues?"***
- ***"Can we establish the main causes of application sideloading? (i.e. third-party marketplaces, privacy, piracy)"***
- ***"Are there any demographic variables which influence these causes? (age, sex, education, nationality)"***

Sideloading research is limited to very few papers and all out-of-date, therefore the research field which has potential for much further exploration. It is certainly possible that the research hypothesis will conclude with definitive causes for sideloading which could further research in aspects of smartphone security and behaviour. Successful identification of these causes could enable similar research models for other devices. Furthermore, research in this area would become heightened if Problematic Smartphone use becomes a clinically recognised behavioural disorder.

6. ABOUT THIS RESEARCH

This PhD is supervised by Dr Sandra Woolley, Prof Fiona Polack and Dr Adam Stanton and is based in Software and Systems Engineering Research in the School of Computing and Mathematics at Keele University.

7. REFERENCES

BBC. (2020). Google warns Huawei owners against 'sideloading' its apps. Available: https://www.bbc.co.uk/news/technology-51613577. Last accessed 24th Feb 2020. Brady, R. (2018). App Sideloading and Cyber Risk. ITNOW, [online] 60(4), pp.46-47. Available at: https://doi.org/10.1093/itnow/bwy103. Last accessed 19 Feb. 2020.

Branwyn, G. (2000). Jargon Watch. Available: https://www.wired.com/2000/03/jargon-watch-59/. Last accessed 8th Feb 2020.

Breitinger, Frank & Tully-Doyle, Ryan & Hassenfeldt, Courtney. (2019). A survey on smartphone user's security choices, awareness and education. Computers & Security. 88. 101647. 10.1016/j.cose.2019.101647.

Gibbs, S. (2016). South Koreans flock to remotenorthern area to play Pokémon Go. Available:https://www.theguardian.com/technology/2016/jul/13/pokemon-go-south-koreans-remote-area-sokcho-google-maps. Last accessed 25th Feb2020.

Global Stats. [online] Available at: http://gs.statcounter.com/osmarketshare/mobile/worldwide Last accessed 13 Feb 2020.

Influence Central. (2016). Kids & Tech: TheEvolution of Today's Digital Natives. Available:http://influence-central.com/kids-tech-the-evolution-of-todays-digital-natives/. Last accessed 13th Feb 2020.

Khan, A. I., Al-Badi, A. and Al-Kindi, M. (2019) 'Progressive Web Application Assessment Using AHP.' Procedia Computer Science. (The 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019), The 14th International Conference on Future Networks and Communications (FNC-2019), The 9th International Conference on Sustainable Energy Information Technology), 155, January, pp. 289–294.

Kirillov, R. (2020). New malware protections for Advanced Protection users. Available: https://www.blog.google/products/android/new-malware-protections-advanced-protection-users/. Last accessed 12th Jul 2020.

Ofcom. (2018). Children and parents: Media useand attitudes report 2018. Available:https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf. Last accessed 18th Feb 2020.

Pewglobal. (2019). Smartphone Ownership IsGrowing Rapidly Around the World, but NotAlways Equally. [online] Available at:https://www.pewglobal.org/wpcontent/uploads/sites/2/2019/02/Pe-Research-Center_Global-

Technology-Use-2018_2019-0205.pdf. Last accessed 13 Feb. 2020.

StatCounter Global Stats. (2019). Mobile Operating System Market Share Worldwide | StatCounter Statista. (2016). Number of network connecteddevices per person around the world from 2003to 2020. Available: https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person/. Last accessed 13th Feb 2020.