Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild

Nissy Sombatruang
University College London

Lucky Onwuzurike
University College London

M. Angela Sasse
University College London, Ruhr University Bochum

Michelle Baddeley
University of South Australia

ABSTRACT

Security experts often question why some users take actions that could expose them to security and privacy risks. Using unsecured Wi-Fi networks is one common example. Even though mobile data is now a more secure means to connect to the Internet, and is becoming faster and more affordable, many users continue to use unsecured Wi-Fi. To identify risk mitigating strategies, the research community first needs to understand the underlying factors driving users' decisions. Previous studies examined stated preferences — what people *said* they have done or *think* they would do — but that may not truly reflect real-life behavior. This study is the first to examine revealed preferences — what people *actually* do in naturalistic settings. Specifically, we investigated how users' desire to save mobile data and battery power influenced their decisions at the time when they connected to open unsecured Wi-Fi in the wild. We also examined whether the decision to use unsecured Wi-Fi networks could be driven by demographic factors and the user's perception of the risk associated with using these networks. We recruited 71 participants in the UK to install *My Wi-Fi Choices*, our own Android app, on their mobile device, and run it for three months in the background. The app captured details of mobile data allowance and battery power on participants' devices whenever they used open unsecured Wi-Fi networks. We found that depleting mobile data significantly drove participants to use these networks, especially when their remaining allowance reached approximately 30%. Battery level, however, did not play a significant role. The perceived risks of unsecured Wi-Fi did not affect the decision-making either. Age, education, and income level were also correlated with increased use of unsecured Wi-Fi.

ACM Reference Format:
Nissy Sombatruang, Lucky Onwuzurike, M. Angela Sasse, and Michelle Baddeley. 2019. Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild. In *Proceedings of Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'19).* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Public Wi-Fi provides easy access to the Internet for many users when needed. In the UK, there are nearly 500,000 commercial Wi-Fi hotspots in 2018, a rapid growth of almost 200% from 2013 [17]. But these networks are often unsecured [6], especially those that do not use encryption, exposing users to security and privacy risks that may arise from websites and applications transmitting sensitive user information in clear text.

Despite growing evidence of these risks — from literature [4, 8, 18, 19, 37–39, 44] and media reports (e.g., [3, 23, 26, 27, 36, 41]) — many people still use potentially unsecured public Wi-Fi [21, 33, 43], even now that mobile data access is becoming faster and cheaper [2, 30]. Understanding why people make such decisions is key to helping us identify appropriate risk mitigating strategies.

Previous studies have investigated various factors, with mixed results. A 2008 study found that users lacked awareness of the risks from using unsecured public Wi-Fi [19]. However, subsequent studies showed that users were aware of the risks [21, 34] but showed optimism bias — that is, they did not believe they would fall victim [42, 43]. More recent studies found that the perceived risks did not affect decision-making but rather it was the users' desire to conserve mobile data that drove them to use unsecured Wi-Fi [38, 39] — an important finding given many people now regularly use mobile data. Demographic factors such as age [21, 30], gender [30, 38, 39], and education level [38] have also been shown to play a role, but this influence was not consistent.

These findings shared one common limitation; they relied on a survey or an interview of stated preferences — what users *said* they have done or what they *think* they would do — which may not truly reflect real-life behavior. Our study is the first to elicit users' revealed preferences — what users *actually* do in natural settings — by examining driving factors at the point when users connected to unsecured Wi-Fi networks in the wild.

Specifically, we first examined whether users could be influenced by the constraint of two resources: mobile data and battery power. The study on how the desire to conserve limited resources — hereafter called *resource preservation heuristic* — affects decision-making is relatively new and not very well-understood, especially in the context of uses of unsecured Wi-Fi; hence, we explored it further. We designed an Android app, *My Wi-Fi Choices*, and recruited 71 participants in the UK to install it on their mobile device with the app running in the background for three months. Whenever participants connected to open unsecured Wi-Fi, the app captured the remaining mobile data allowance and battery level on their devices, allowing us to observe how resource preservation heuristic influenced decision-making. We also examined whether the perceived

WiSec'19, May 15–17, Miami, FL, USA
© 2019 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

risks of using these networks and demographic factors played a role in participant's choices.

Our findings gave new insights. Participants did not value all resources equally. Depleting mobile data — especially when levels reached 30% — had a significant effect in driving participants to use unsecured Wi-Fi, but depleting battery level did not have a similar impact. We also obtained evidence that perceived risks of unsecured Wi-Fi did not affect participants' decision-making. Some demographic factors played a role but these effects were inconsistent.

Knowledge gained from our study can help to design workable risk mitigating strategies. Particularly, it suggests that risk mitigating strategies that do not rely on the users alone are needed. Limited mobile data allowances will continue to drive users to use unsecured Wi-Fi networks. Encouraging application developers and public Wi-Fi providers to encrypt transmitted data is a more promising approach.

Contributions. Overall, we make the following contributions in this study:

- We designed and implemented *My Wi-Fi Choices*, an Android app that allowed us to collect and analyze user resources at the point when they connected to unsecured Wi-Fi rather than relying on a survey or an interview.
- We showed that mobile data preservation heuristic played a significant role in driving users to use unsecured Wi-Fi. While the results of the study could be considered intuitive and unsurprising, our study is the first to provide empirical evidence to support this notion.
- We showed that user perception of risks relating to unsecured Wi-Fi did not affect their decision-making, and demographic factors played less of a role.

The rest of the paper is structured as follows: Section 2 outlines related work. Section 3 introduces our data collection technique and the statistical analysis we performed. We present the results in Section 4 and discuss the implication of our findings, the limitations of our work, and possible future work in Section 5 before concluding in Section 6.

2 RELATED WORK

In this section, we reviewed prior work that examined the security and privacy risks of unsecured Wi-Fi networks, uses of these networks, and the factors influencing users' decisions to use them.

2.1 Security and privacy risks of unsecured Wi-Fi networks

Data transmitted via unsecured Wi-Fi networks are exposed to many security and privacy risks — from eavesdropping [18, 19] to man-in-the-middle attack [4, 8, 37]. Numerous media have reported on the risks these networks expose users to (e.g., [3, 23, 26, 27, 36, 41]).

Previous studies have also provided supporting evidence. In 2012, Cheng *et al.* [9] showed that private information of two thirds of travelers were leaked when they used public Wi-Fi at 15 airports in 4 countries — worrying, given that many travellers rely on public Wi-Fi, especially when travelling overseas. F-Secure [13], a security company, set up a free open unsecured Wi-Fi network in London in 2014 and captured one login credential transmitted in clear text. Sombatruang *et al.* [39] performed a similar experiment in 2016, also in London, and found private information such as date of birth and sexual orientation being transmitted from a dating app without any encryption. Their subsequent study in 2017 in Japan showed more alarming evidence; sensitive information such as private emails, login credentials, and business transactions were transmitted in clear text [38]. While users may be aware of the risks of entering private information on unencrypted webpages (i.e., those served over HTTP) on a browser and may abstain from doing so, the same cue is not visible to the users on non-browser-based applications (apps), and their use of these apps may expose them to additional risks they may not be aware of. Prior work has shown that some non-browser apps transmit sensitive user information in clear text [14, 31]. Hence, this information can be easily retrieved by an eavesdropper listening on the unsecured Wi-Fi that users connect to.

2.2 Uses of unsecured Wi-Fi networks

Empirical evidence of unsecured Wi-Fi risks is worrying — not only because many applications do not encrypt transmitted data but also because people continue to use the networks. This phenomenon may seem surprising, given that mobile data, an alternative option to connect to the Internet, is becoming cheaper and faster. However, Action Fraud [2], the UK national fraud and cyber-crime reporting center, reported that 76% of people in the UK with a mobile data subscription in 2016 still use public Wi-Fi. Ofcom [30] reported a smaller percentage, 67%, in 2017 — still considerably high given two in three people could have had their data compromised when using these networks.

Avast [33], a security company, set up a fake open unsecured public Wi-Fi at a political convention in the US in 2016 and found 1,200 users connected to it — of which 44.5% used the networks for emails and instant messaging. McShane *et al.* [21] also found that 58% of public Wi-Fi users in Australia admitted to have used free open unsecured networks in the past three months prior to the survey — worrying, given that more than half of the participants could have had their data exposed. The recent 2017 Norton Global Wi-Fi Risks Report highlighted that more than half of their 15,532 survey participants from 15 countries were unable to resist using free public Wi-Fi and 80% admitted using these networks to make sensitive information such as email and online banking [43].

2.3 Factors affecting users' decision to use unsecured Wi-Fi

Previous studies have examined both proximal and distal factors influencing decision-makings. Proximal factors affects decision-making in immediate situations while distal factors play a role from a greater distance.

2.3.1 Proximal factors. Several proximal factors contribute to why users continue to use unsecured Wi-Fi. Klasnja *et al.* [19] interviewed 11 participants and found that they did not understand the risks of using public Wi-Fi. However, the study was conducted in 2008 when the risks of unsecured Wi-Fi networks were less publicized. More recent studies have showed that users are becoming more knowledgeable. McShane *et al.* [21] found that about two-thirds of their participants viewed public Wi-Fi networks as unsecured. Seigneur *et al.* [34] also found that only 10% of their 1,743 survey participants did not know about the risks and the existence of fake public Wi-Fi. These findings all point in the same direction; most users are aware of the risks. But why they still use the networks is puzzling.

Optimism bias — often known as a false sense of security — may help to explain why users continually use unsecured Wi-Fi even when they are aware of the risks. Swanson *et al.* [42] found that users of public Wi-Fi did not believe the risks would be realized. Symantec [43] resonated the message — reporting that 60% of survey participants felt that their personal data were safe when using public Wi-Fi, of which 15% said they felt very safe. Klasnja *et al.* [19] also found that participants relied on the security of their devices to mitigate the risks when using public Wi-Fi.

Another factor that plays a significant role, but had been under examined until recently, is the constraint of mobile data allowance. McShane *et al.* [21] found that only one in ten of their survey participants preferred using mobile data over public Wi-Fi; however their study did not explore how the users' preferences changed as mobile data allowance depleted. Sombatruang *et al.* [38, 39] addressed this gap in the literature. Using a series of hypothetical scenarios, they found that participants displayed a resource preservation heuristic tendency — saying they were willing to use public Wi-Fi to save mobile data, especially when the data allowance reached 25%, the lowest end in the scenarios. However, their findings were based on a survey of participants' stated preference. We addressed this gap and examined user-generated data in naturalistic settings. We also examined whether the remaining battery power of users' devices affected their decisions to use unsecured Wi-Fi as Wi-Fi generally consumes less energy than does mobile data [16, 47]. Vaniea and Rashidi [45] showed that some users were reluctant to update software because they believe it would drain the battery — even though the update could mitigate security risks. We put this hypothesis to the test in the context of using unsecured Wi-Fi networks.

The effects of resource preservation on decision-making has its root in psychology and economic literature. Previous studies showed that the constraints of resource — be it financial related or time — taxed cognitive bandwidth needed to think clearly and make optimal decisions [20, 25, 35, 40, 46]. Shah *et al.* [35] showed how the lack of money influenced poor participants[1] to make riskier suboptimal financial decisions; it introduced cognitive load and interfered with participants' ability to judge a situation effectively.

Findings from Mani *et al.* [20]'s lab and fieldwork experiment echoed the findings from Shah *et al.* [35]. In the lab experiment, they observed poor cognitive performance among the poor but not the rich participants[2] after asking them to think about situations of financial difficulty. Their experiment in India also supported the theory, showing that the cognitive performance of the same sugarcane farmers before the harvest season — when most farmers experienced financial difficulties — was worse than their performance after the harvest season — when farmers started earning. They concluded that, before the harvest, the farmers' attention was diverted toward concern about financial difficulties. Similar behavior was observed in another study which found that participants assigned to choose 1-2 household items for free prior to taking cognitive tests did worse than participants assigned to choose more free items [40]. Having a small budget appeared to tax cognitive bandwidth and impede cognitive performance.

These evidence clearly shows that resource constraints triggered intrusive thoughts and tax cognitive bandwidth, leading to impeded cognitive performance and sub-optimal decision-making [25, 46]. This theory may help to explain the findings in the study of Sombatruang *et al.* [38, 39] which found users having limited mobile data allowance displayed a risk-taking attitude and said they would use unsecured Wi-Fi when mobile data allowance was running low; an intrusive thought about running out of data taxed their mind and blinded them from potential ramifications.

2.3.2 Distal factors. Previous studies also found some demographic factors affected the use of unsecured Wi-Fi networks. But the findings were mixed. Ofcom [30] reported more males than females in the UK used public Wi-Fi networks. However, Sombatruang *et al.* [38, 39] found the opposite. Age has also been reported to play a role. Young people (18-24 years old) in the UK and in Australia used public Wi-Fi more frequently than other age groups [21, 30], which is unsurprising given the influence of social media nowadays. Sombatruang *et al.* [38] also found that education level affected decision-making among the Japanese; people holding a bachelor's or post-graduate degree were less likely to use public Wi-Fi than others with lower levels of education.

3 METHODOLOGY

In this section, we introduce the data collection technique, statistical analysis, and the ethical considerations of our study.

3.1 Data collection

3.1.1 My Wi-Fi Choices app. To examine the influence of mobile data and battery power on the use of open unsecured public Wi-Fi networks, we developed an Android app, *My Wi-Fi Choices*, which collected the actual battery level and the estimated remaining mobile data allowance on a participant's mobile device whenever they connected to open unsecured public Wi-Fi networks. For this study, we defined such networks as those requiring no key exchange session when a device connects to it; hence, providing no encryption

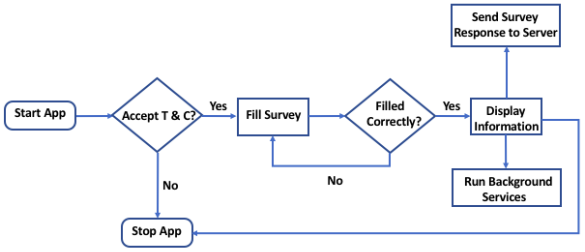


Figure 1: An overview work flow of *My Wi-Fi Choices*.

[1] Randomly assigned as poor or rich as part of the experiment.
[2] Poor participants classified as having real-life earnings in the lower quartile of the U.S. income distribution.

or authentication. From a user interface perspective, they are networks without a security padlock icon next to the Wi-Fi bar on the screen showing a list of available Wi-Fi networks.

My Wi-Fi Choices operates in two modes: foreground (i.e., the activities of the app are visible to the user) and background (i.e., the app runs as a service and is not visible to the user). We show in Figure 1, an overview of the work flow and in the following paragraphs, describe the details of each mode and the data collection techniques.

Foreground Mode. *My Wi-Fi Choices* runs in the foreground in all its operation where user input is required. When participants installed and ran the app for the first time, they were asked to agree to the terms and conditions of our app. Once they agreed, they were asked to complete a survey (see Appendix A) where they had to supply their mobile data plan (e.g., 1 GB per month) and the renewal date. These initial values were used to calculate an estimated remaining data allowance. The app also asked participants to supply demographic info such as gender, age group, and education level and their perceived risks of data breach when using public Wi-Fi and mobile data (on a scale of 0% to 100%, 0% being not very likely and 100% being very likely). These data allowed us to evaluate our hypothesis on the factors that affect participants' use of unsecured Wi-Fi networks.

Background Mode. When *My Wi-Fi Choices* runs in background mode, it runs `services`, while also listening for selected `broadcasts`. In particular, after a successful completion of the survey questions, it starts four `services`. The first `service` which is a `FirebaseInstanceIdService` is used to generate tokens that we use to uniquely identify each participant, while the second `service` is a messaging service that handles notifications sent from our server to the app. The third `service` registers a CONNECTIVITY_ACTION `BroadcastReceiver` that is used to monitor changes in Internet connectivity. Starting a service to register a `broadcast` is necessary because "apps targeting Android 7.0 (API level 24) and higher do not receive the CONNECTIVITY_ACTION broadcasts if they declare the broadcast receiver in their manifest"[3]. Hence, we use this method as a workaround to monitor when a device connects to a network. Finally, the fourth `service` is responsible for collecting the data we use in our experiment.

Similarly, in this mode, the app registers three `BroadcastReceivers` that respectively listens for changes in Internet connectivity (this is registered by a `service` as stated earlier), device boot completion, and low battery level. We listen for changes in Internet connectivity so as to track when a user connects to unsecured Wi-Fi. Whereas we track device boot completion and low battery level, so as to simultaneously restart the `services` and collect data when the battery is low if the device is running Android versions lower than 6.0 (we explained why the app acts differently by Android version).

Data Collection Technique. To evaluate how much of a user's data is remaining from their data plan when they connect to unsecured Wi-Fi, we subtract the amount of data they have used from the data they subscribed to. To deduce how much data a user has used, we do so following two approaches depending on the Android version on the device. When a device is running Android version 6.0 or higher, we read the mobile data already exhausted using the `NetworkStatsManager` class[4]. The class provides access to network usage history and statistics which can be used to get network usage history for a given `bucket` i.e., time window e.g., one month for monthly data plan cycle. Usage of this class requires API level 23 or higher (i.e., Android version 6 or higher) and a system-level permission; thus, if a user refuses to grant our app the required permission, we use the second approach to get the amount of data already exhausted.

When a device runs an Android version lower than 6.0, we get the data already exhausted using the `TrafficStats` class[5]. The network traffic statistics (stats) provided by this class is reset after every reboot by the OS, hence, its historical statistics is not as robust as that provided by `NetworkStatsManager`. Therefore, to get network stats that are almost accurate, we start a `service` that reads and saves the network stats every hour as a user may turn their device off at any time. We also register a `BroadcastReceiver` that listens for low battery level and reads and saves the network stats when the battery is low. In the same vein, if a device is not rebooted during the period of our experiment, we reset the saved network stats to zero at the end of a user's data plan cycle (e.g., monthly).

To read the battery level of a device, we use the `BatteryManager` class[6]. Note that we only collect data when a user connects to unsecured Wi-Fi. To distinguish between secured and unsecured Wi-Fi, we examine the capabilities of the access point a user is connected to. We consider a Wi-Fi network to be unsecured if it is not encrypted e.g., using WPA or WEP. Finally, we send the data to our server (an Amazon EC2 Ubuntu machine) via HTTPS only and we also employ certificate pinning[7] to prevent man-in-the-middle attacks.

The data collection took place for 3-months, starting from the date when the participant installed the app. It commenced in July 2017 and ended in December 2017.

3.1.2 *Recruitment and participants.*

We advertised our study using both offline and online media to increase participant diversity. For the former, we put flyers on 24 notice boards around the city. These locations included university campuses, coffee shops, business offices, grocery stores, charity shops, local public libraries, and construction sites. For the online channel, we advertised the study via both the university-wide and the department's student mailing lists, the university web site, Twitter accounts from two of the university's departments, and Callforparticipants.com.

Interested participants were asked to fill out an online prescreening test. Eligible participants were restricted to only individuals living in the UK who are 18 years old or above, all of whom have an Android device (minimum OS version 5.0) with a mobile data plan, and had used public Wi-Fi networks from time to time, according to their responses to the self-assessed pre-screening questions.

[3] https://developer.android.com/training/monitoring-device-state/connectivity-monitoring.html

[4] https://developer.android.com/reference/android/app/usage/NetworkStatsManager.html

[5] https://developer.android.com/reference/android/net/TrafficStats.html

[6] https://developer.android.com/reference/android/os/BatteryManager.html

[7] https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

We sent the eligible participants a link to the Google Play Store to download *My Wi-Fi Choices*. Participants were allowed to install the app any time upon receiving the invitation, provided they did so before the end of September 2017 when we removed the app from the store. Each participant received up to a £20 reward for their participation (£10 after two months and another £10 at the end of the third month after installing the app). A total of 71 participants were recruited. Participants encompassed a diverse demographic such as age, gender, and education level (see Appendix B).

3.2 Statistical analysis

To allow us to make an inference about general population from the samples in our study, we applied six statistical analyses: polynomial regressions, Cochran's Q Test, Student's T-Test, Levene's Test, Pearson's correlation coefficient, and binary logistics regression.

Polynomial regressions allowed us to build models of how participants connected to unsecured Wi-Fi at different point in their mobile data allowance and battery power. These best fitting models, created based on actual data, have several benefits. First, they helped us to address our main research questions — whether use of unsecured Wi-Fi networks could be influenced by the constraints of resources, and, if so, at which point did they prompt user decisions. The holistic view of the models also makes it easy for readers to visualize and interpret the results. Moreover, the models are useful for predicting the outcome given a set amount of input data from a different data set. In our study, as an example, given the remaining mobile data allowance, we could forecast the likelihood of mobile phone subscribers from a particular carrier to use unsecured Wi-Fi when their data allowance reaches 25%. The best fitting models are also commonly used when putting all data points in a graph would make the graph incomprehensible.

We used Cochran's Q Test, an appropriate test for our data type, to examine whether the changes observed among data points in the polynomial regression models were statistically significant. We used Student's T-Test to determine whether the perceived likelihood that unsecured Wi-Fi could be compromised between participants connecting to and not connecting to the networks were statistically different. Levene's Test was for testing the homogeneity of variances needed in Student's T-Test. Pearson's correlation analyzed whether the frequency of using unsecured Wi-Fi could be influenced by the perceived risks of using the networks. Finally, binary logistics regression predicted the probability of participants using — or not using — unsecured Wi-Fi networks based on their demographic factors. More details of each test are in Section 4. We used SPSS to run all analysis.

3.3 Ethics approval

We submitted the study design to the Ethics Chair Actions (part of the IRBs of the institution in the UK) prior to commencing the fieldwork. We were granted permission for the study provided: 1) we collected data anonymously and explained the study to the participants and received consent from them; 2) we complied with applicable data protection laws. Our app did not collect any personally identifiable information. We informed participants about the study during the recruitment and included an information sheet in the app that participants could refer to at any time. Participants were also presented with a consent form and terms and conditions on the first screen when they installed the app. We instructed each participant via a notification to uninstall our app at the end of the experiment. We also shut down our server at the end of the experiment to prevent collecting data from participants who may have forgotten to uninstall the app. To promote security and privacy, we encrypted the data we collected from participants both in transit and at rest. Our server was located in the UK. We will delete the data upon publication of the study.

4 RESULTS

In this section, we present the results from examining factors influencing users to use unsecured Wi-Fi.

4.1 Mobile data preservation heuristic

To examine how the constraints of mobile data allowance influenced the use of unsecured Wi-Fi networks, we investigated whether more participants would use the networks as their data allowance depleted.

First, we ran a polynomial regression using a cubic model (equation 1) to examine the relationship between the uses of unsecured Wi-Fi and the remaining data allowance. The model enabled us to determine the optimal point at which participants displayed risk-taking behavior by using unsecured networks. We chose the cubic model as it best fitted our dataset, showing a larger Nagelkerke R^2 value[8] than the linear and quadratic model.

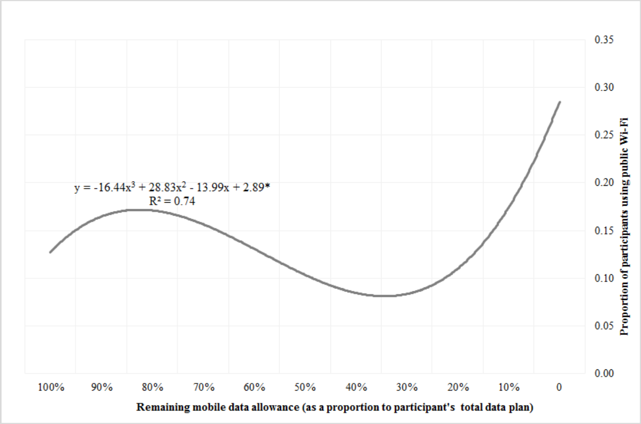
$$y = ax^3 + bx^2 + cx + d \tag{1}$$

Where y is the proportion of participants that uses unsecured Wi-Fi networks; x is the percentage of remaining mobile data allowance on a 10% interval scale; a, b, and c are the coefficients; and d is the constant.

The model showed that early in the mobile data plan cycle, an increasing proportion of participants used unsecured Wi-Fi networks as their mobile data allowance depleted from 100% to 80% (Figure 2). From this point onward, a decreasing proportion of participants used unsecured Wi-Fi. This trend continued until the remaining data allowance reached around 30%, when a change of direction emerged. More participants connected to unsecured Wi-Fi from that point onward and at an accelerated rate — suggesting that 30% is an optimal point at which participants displayed risk-taking behavior in order to preserve mobile data allowance. This optimal point is close to the 25% level identified in previous studies [38, 39]. However, our results are based on revealed preference, a closer proxy to naturalistic behavior than the stated preferences in the two previous works.

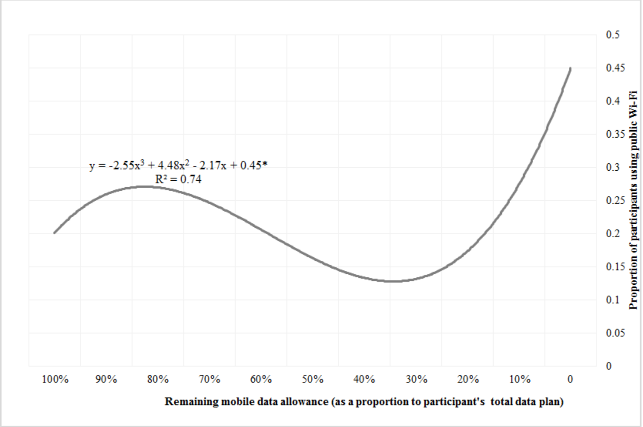
Our dataset showed that some participants did not connect to any unsecured Wi-Fi networks during the experiment. This could be because they were using less-frequently used devices to take part in our study or they connected to secure Wi-Fi at their workplace and at home only. Hence, to take a conservative approach, we ran another regression with these participants excluded. Despite the differences in the coefficients and constant, the model showed a similar trend (Figure 3). The 30% remaining data allowance was still

[8] The R^2 determined the percentage of variation in the dependent variables that was explained by the model.



*Significant at $p < 0.05$, $n = 71$

Figure 2: Changes in the proportions of participants using unsecured Wi-Fi networks as their data allowance depleted.



*Significant at $p < 0.05$, $n = 45$

Figure 3: Changes in the proportions of participants who used unsecured Wi-Fi networks as their data allowance depleted (excluding participants who did not use these networks during the experiment)

a tipping point at which participants displayed risk-taking behavior and turned to unsecured Wi-Fi networks.

We also ran a Cochran's Q Test (equation 2) to analyze whether the differences in the observed proportions of participant using unsecured Wi-Fi networks as the mobile data allowance depleted were statistically significant. We checked that our data met the four assumptions needed for Cochran's Q Test[9].

$$T = k(k-1)\frac{\sum_{j=1}^{k}(X_j - \frac{N}{k})^2}{\sum_{i=1}^{b} X_i(k - X_i)} \tag{2}$$

Where k is the proportion to be observed (i.e. the remaining mobile data allowance on a scale of 10% interval from 1.0, 0.9,...,to 0.0); b is the number of participants; X_j is the column total for the j^{th} proportion; X_i is the row total for the i^{th} proportion; and N is the grand total.

The Cochran's Q test determined that the differences observed were statistically significant for both analyses i.e., including and excluding participants who did not connect to any unsecured Wi-Fi networks during the experiment ($x^2(10) = 32.29, p < 0.001$).

We further analyzed whether participants with unequal sized data plan (i.e., a small vs a large data plan) would exhibit the same behavior. We classified participants having at least 3 GB/month and less than 3 GB/month, as the *Data Rich* and the *Data Poor*, respectively[10]. This 3 GB/month cut-off was the median in the data set. We also considered it large enough for an ordinary user to not be too worried with preserving mobile data.

We found that the remaining data allowance of 30% remained the optimal point at which both the *Data Rich* and the *Data Poor* leaned towards using unsecured Wi-Fi networks. More of the *Data Rich* than the *Data Poor* used open unsecured public Wi-Fi networks (Figure 4). The differences observed among the proportion of participants using unsecured networks as the data allowance depleted were statistically significant among the *Data Rich* ($x^2(10) = 28.41$, $p < 0.01$) but not among the *Data Poor* ($x^2(10) = 10.97, p > 0.05$) — suggesting that the differences among the latter could be due to chance. But these results included participants who did not use any unsecured Wi-Fi during the experiment. Again, considering the possibility of participants using infrequently used devices in the study or only connecting to secure Wi-Fi at their workplace and at home, we undertook a conservative approach and ran another regression — excluding participants that did not use unsecured Wi-Fi during the experiment. The median value of mobile data plans became 4 GB/month; hence, the *Data Rich* had at least 4 GB/month and the *Data Poor* had less.

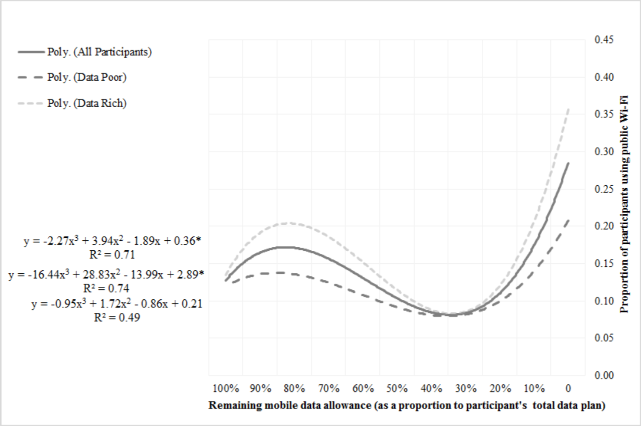
We observed that the 30% optimal point at which the *Data Rich* displayed risk-taking behavior and used unsecured Wi-Fi networks remained unchanged (Figure 5). However, the optimal point of the *Data Poor* now shifted from 30% to 40% — suggesting they were more sensitive to the resource preservation heuristic than the *Data Rich*. In addition, more of the *Data Poor* than the *Data Rich* used unsecured Wi-Fi networks after the optimal point. The changes in the proportion of participants were also statistically significant for both the *Data Rich* ($x^2(10) = 22.56, p < 0.05$) and the *Data Poor* ($x^2(10) = 18.31, p < 0.05$).

4.2 Battery power preservation heuristic

To examine whether the constraints of battery power on mobile devices influenced the use of unsecured Wi-Fi networks, we investigated whether more participants would use the networks as the battery depleted.

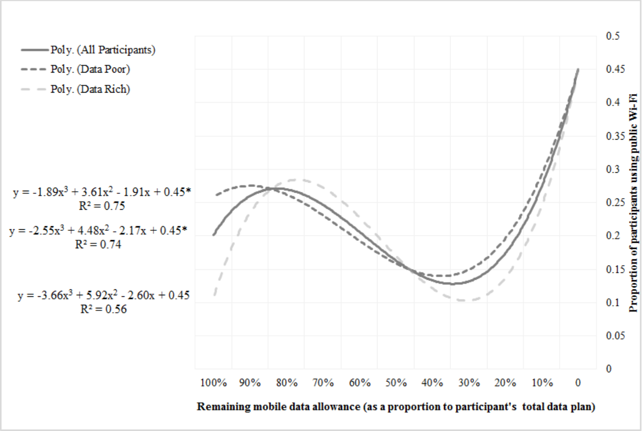
[9] 1. One dependent variable with two possible dichotomous outcomes (i.e. using unsecured Wi-Fi (1) or not using the networks (0)), 2. Three or more categorical related groups (i.e. remaining data allowance on a 10% interval scale from 100% to 0%), 3. Randomly selected samples, 4. Sufficiently large sample size ($n = 71$ for total population, $n = 45$ excluding participants who did not use any unsecured Wi-Fi networks during the experiment).

[10] Participants on a pay-as-you-go plan were classified as *Data Poor*.



*Significant at $p < 0.05$, $n = 71$

Figure 4: Changes in the proportion of the *Data Rich* and the *Data Poor* using unsecured Wi-Fi networks as their data allowance depleted.



*Significant at $p < 0.05$, $n = 45$

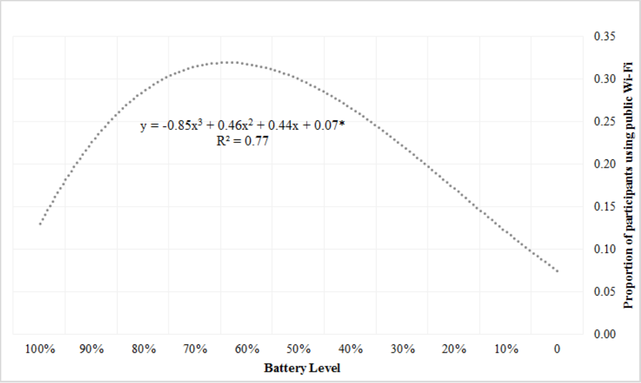
Figure 5: Changes in the proportion of the *Data Rich* and the *Data Poor* using unsecured Wi-Fi networks as their data allowance depleted (excluding participants that did not use these networks during the experiment)

We ran a similar polynomial regression using a cubic model (equation 3) which also best fitted our dataset.

$$y = ax^3 + bx^2 + cx + d \tag{3}$$

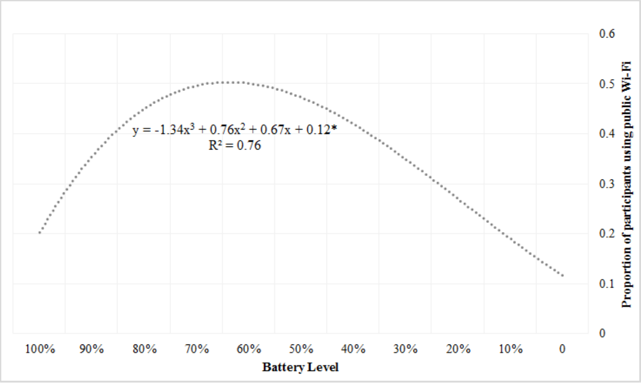
Where y is the proportion of participants that decides to use unsecured Wi-Fi networks; x is the percentage of remaining battery level on a 10% interval scale; a, b, and c are the coefficients; and d is the constant.

The model produced a bell-shaped curve shown in Figure 6. As the battery depleted, an increasing proportion of participants connected to unsecured Wi-Fi networks but that trend stopped when the battery reached approximately 60%. From that point onward, the curve turned downward; fewer participants used the networks.



*Significant at $p < 0.05$, $n = 71$

Figure 6: A cubic model of changes in the proportion of participants using unsecured Wi-Fi networks as their device battery level depleted



*Significant at $p < 0.05$, $n = 45$

Figure 7: A cubic model of changes in the proportion of participants using unsecured Wi-Fi networks as their device battery level depleted (excluding participants who did not use these networks during the experiment)

Excluding participants who did not connect to any unsecured Wi-Fi networks during the experiment produced a similar bell-shape curve (Figure 7). This could possibly be due to participants not using their devices once their battery level reached a certain level. Nonetheless, the Cochran's Q test determined that the differences in the proportions of participants using unsecured networks as the battery level depleted were statistically significant for both analyses ($x^2(10) = 56.95$, $p < 0.001$). Therefore, there was sufficient evidence to reject the hypothesis that as the battery level depleted, more participants would used unsecured Wi-Fi networks.

4.3 Perceived risks of using unsecured Wi-Fi networks

We examined whether the participants' perceived likelihood that public Wi-Fi can be compromised (on a scale of 0% to 100%, 0% being least likely and 100% being most likely) affected their usage of unsecured Wi-Fi. We considered public Wi-Fi a reasonable proxy of unsecured Wi-Fi networks. We also relied on previous works which evaluated users' understanding of the privacy and security risks of using public Wi-Fi today [21, 34].

We first analyzed the mean difference in the perceived risks between participants who did not use any unsecured Wi-Fi and those that connected at least once during the experiment. We hypothesized that participants that used unsecured Wi-Fi would rate the risk lower. We ran an independent sample T-Test for equal (equation 4.1) and unequal (equation 4.2) variances to evaluate whether the observed difference in the mean was statistically significant. We checked that our data met the assumptions required for the T-Test[11]. We also used the Levene's Test [12] for equality of variances to determine whether the data sets were subjected to (equation 4.1) or (equation 4.2) — a statistically significant result ($p > 0.05$) assumed equal variances and would be subjected to (4.1).

$$t = (\mu_1 - \mu_2)/\sigma_p \sqrt{1/n_1 + 1/n_2} \tag{4.1}$$

$$t = (\mu_1 - \mu_2)/\sigma \sqrt{\sigma_1^2/n_1 + \sigma_2^2/n_2} \tag{4.2}$$

Where μ_1 is the mean risk of using public Wi-Fi as perceived by participants that used unsecured Wi-Fi networks at least once during the experiment; μ_2 is the mean risk as perceived by participants that did not use unsecured networks during the experiment; n_1 is the number of participants that used unsecured Wi-Fi network at least once during the experiment; n_2 is the number of participants that did not use unsecured networks during the experiment; σ_p is the pooled standard deviation of the total population; σ_1 is the standard deviation of n_1; and σ_2 is the standard deviation of n_2.

We found that participants that used unsecured Wi-Fi networks at least once during the experiment rated the risk lower than those who did not ($\mu_1 = 58.33$, $\mu_2 = 64.92$). However, the difference was statistically insignificant ($t(69) = -0.94$, $p = 0.35$), suggesting it could be due to chance.

We then analyzed whether the frequency of using unsecured Wi-Fi could be influenced by the perceived risks of using the networks. We examined Pearson's correlation coefficients (equation 5) between these two variables. We checked that our data sets met the assumptions[13] required for Pearson's correlation test.

$$P_{x,y} = cov(x,y)/\sigma_x \sigma_y \tag{5}$$

Where *cov* is the covariance; σ_x is the standard deviation of the participants' frequency of using unsecured Wi-Fi networks during the experiments; and σ_y is the standard deviation of the participant's perceived likelihood that public Wi-Fi can be compromised.

We found a negative correlation between the perceived risks of using public Wi-Fi and the frequency of using unsecured Wi-Fi networks. As the perceived risks increased, the frequency decreased. However, the correlation was statistically insignificant ($r = -0.05$, $n = 71$, $p = 0.67$). Excluding participants that did not connect to unsecured Wi-Fi during the experiment also showed an insignificant negative correlation ($r = -0.02$, $n = 5$, $p = 0.91$). We found a mix of positive and negative correlations among the *Data Rich* and the *Data Poor* but none were statistically significant either (Table 1).

Table 1: Pearson's correlation between the frequency of using unsecured Wi-Fi networks and the perceived risks. (Including/excluding participants that did not connect to any unsecured Wi-Fi network during the experiment.)

Parameter	Including		Excluding	
	Data Rich	Data Poor	Data Rich	Data Poor
r	-0.03	-0.08	0.02	-0.02
n	37	34	17	28
p	0.87	0.65	0.93	0.93

These findings provided sufficient evidence to reject the hypothesis that the perceived risks of unsecured Wi-Fi networks affect the decision to use these networks. They also supported the findings of prior work [38], which observed similar behavior among the Japanese.

4.4 Demographic Factors

We ran binary logistic regressions (equation 6) which predicted the probability of participants using — or not using — unsecured Wi-Fi networks based on demographic factors such as age, gender, employment status, etc. This type of regression is generally used to test whether an observation falls into one of two values of a dichotomous dependent variable based on the independent variables. We checked that our data met the four assumptions[14] needed for the regressions and analyzed the Nagelkerke R^2 values.

$$Pr(Y_i = 1|X_i = x_i) = exp(\beta_0 + \beta_1 x_i)/(1 + exp(\beta_0 + \beta_1 x_i)) \tag{6}$$

Where Y is a binary response variable, $Y_i = 1$ if a participant used an unsecured Wi-Fi network, $Y_i = 0$ if a participant did not use the network, $X = (X_1, X_2, ..., X_k)$ is the independent variable (i.e. gender, age group, education, employment status, and income level).

We found statistically significant correlations between age, education, income, and the use of unsecured Wi-Fi networks at various remaining data allowance and battery intervals. But no consistent pattern emerged.

4.4.1 Age. When the remaining data allowance was at 40% and 90%, participants aged 26-35 were 0.06 times ($\beta = -2.84$, $OR = 0.06$, $p < 0.05$, $R^2 = 0.30$) and 0.05 times ($\beta = -2.98$, $OR = 0.05$, $p < 0.05$, $R^2 = 0.64$) less likely to use unsecured Wi-Fi networks compared to participants aged 18-25 (the reference group). Moreover, at the 50% battery level, participants aged 26-35 were 0.10 times ($\beta = -2.27$, $OR = 0.10$, $p < 0.05$, $R^2 = 0.29$) less likely to use unsecured Wi-Fi networks than the reference group. At the 80% battery level,

[11] 1. Dependent continuous variables (i.e. the perceived risks on a scale of 0 to 100%), 2. Independent variable has two categorical independent groups (i.e. used or did NOT use unsecured Wi-Fi), 3. Independence of observations, 4. No significant outliers, 5. Normally distributed independent variables, 6. Homogeneity of variances (tested and corrected by the Levene's Test)

[12] Automatically generated by SPSS in the independence samples T-Test.

[13] 1. Two continuous variables (i.e. the perceived risks on a scale of 0 to 100% and the frequency of using unsecured Wi-Fi), 2. Linear relationship between the two variables, 3. No significant outliers, 4. The two variables were normally distributed.

[14] 1. One dependent dichotomous variable (i.e. used or did NOT use unsecured Wi-Fi, 2. At least one independent variable (e.g., gender, education level, etc.), 3. Independent variables were mutually exclusive and exhaustive categories, 4. A linear relationship between any continuous independent variable and the logit transformation of dependent variable (not applicable as our predictors were categorical).

participants aged 36-65 were 236.35 times ($\beta = 5.47$, $OR = 236.35$, $p < 0.05$, $R^2 = 0.46$) more likely to do so. When we excluded participants that did not use any unsecured Wi-Fi networks during the experiment, participants aged 26-35 were 0.003 times ($\beta = -5.99$, $OR = 0.003$, $p < 0.05$, $R^2 = 0.46$) less likely to use unsecured Wi-Fi networks, and participants aged 36-65 became 3,278.36 times ($\beta = 8.10$, $OR = 3,278.36$, $p < 0.01$, $R^2 = 0.67$) more likely. This finding contradicted the survey by Ofcom [30], which reported that more younger (age 18-24) than older people used public Wi-Fi. Perhaps, the latter group said they had used or thought they would use less public Wi-Fi than they usually did in real-life.

4.4.2 Education. We did not find significant correlation between the use of unsecured Wi-Fi and education level at any remaining mobile data interval. This supports the findings from previous work examining stated preferences of factors influencing users to use public Wi-Fi in the UK [39] but contradicts the findings from a similar study in Japan, pointing the likely cause being late exposure to cyber security awareness which usually only starts at university level in Japan [38]. In relation to battery level, however, compared to participants with a bachelor's degree (reference group), participants having postgraduate degree were 0.05 times ($\beta = -3.00$, $OR = 0.05$, $p < 0.05$, $R^2 = 0.46$) less likely to use unsecured Wi-Fi networks when the remaining battery was 80%. When excluding participants who did not use any unsecured Wi-Fi networks during the experiment, the odds reduced to 0.02 times ($\beta = -3.80$, $OR = 0.02$, $p < 0.05$, $R^2 = 0.67$).

4.4.3 Income. We did not find significant correlation between the use of unsecured Wi-Fi and income level at any remaining mobile data interval. The results were counter-intuitive but one possible explanation is that the level of income is not always a proxy for mobile data allowance. Some people with lower income may have larger data plan than some high earners do. For instance, students frequently using social media and/or constantly using instant messaging are likely to have a large mobile data plan, despite having a low income, and use less public Wi-Fi. A previous study also showed that being *Data Poor*, that is, having a small mobile data allowance, is a more influential factor [38]. Other possible explanations are micronumerosity or multicollinearity inflating the standard errors of the parameter estimates and thereby lowering the power of the hypothesis tests.

However, in relation to battery level, high-income participants were more likely to use unsecured Wi-Fi networks than basic-income participants (reference group)[15]. When the remaining battery was 30%, 40%, and 70%, high-income participants were 15.20 times ($\beta = 2.72$, $OR = 15.20$, $p < 0.05$, $R^2 = 0.34$), 13.52 times ($\beta = 2.60$, $OR = 13.52$, $p < 0.05$, $R^2 = 0.36$), and 15.99 times ($\beta = 2.77$, $OR = 15.99$, $p < 0.05$, $R^2 = 0.36$), respectively, more likely to use unsecured Wi-Fi networks. When we exclude participants that did not use unsecured networks during the experiment, high-income participants were 81.14 times ($\beta = 4.40$, $OR = 81.14$, $p < 0.05$, $R^2 = 0.47$) and 29.73 times ($\beta = 3.39$, $OR = 29.73$, $p < 0.05$, $R^2 = 0.46$) more likely to use the networks when the remaining battery was 40% and 50%, respectively.

5 DISCUSSION

In this section, we discuss how we can apply the knowledge from this study, the limitations of the study, and possible future work.

5.1 Applications

The main findings of our study are that the mobile data preservation heuristic plays a significant role in influencing users to use unsecured Wi-Fi networks, and that users are unlikely to stop using these networks, especially when they are running low on their data allowance. This insight, the first to be drawn from empirical evidence of revealed preferences, offers several potential benefits.

First, advising users to stop using public Wi-Fi is likely to be ineffective. Policy makers may consider revising advice such as "*Use mobile data services such as 4G in preference to public Wi-Fi wherever possible.*" — Action Fraud UK [2], "*The simplest precaution is not to connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security.*" — The National Cyber Security Centre (NCSC) [28], or the Football Association (FA) asking England players and staff not to use public or hotel Wi-Fi at the 2018 World Cup in Russia [10]. This advice would have been long forgotten when the data allowance is running low. The resource preservation heuristic would take over and blind users from potential ramifications.

Awareness programmes aiming to increase the perceived risks of using unsecured Wi-Fi networks may not work either. We showed that the perceived risks of using unsecured Wi-Fi networks did not significantly affect the uses of these networks. Policy makers may consider placing a greater emphasis on encouraging the use of a Virtual Private Network (VPN). However, this solution has its own challenges. The adoption rate is relatively low. Norton reported in 2016 that 16% of people in the UK used a VPN when using public Wi-Fi [29] and later in 2017 that 25% of their 5,532 survey participants from 15 countries did the same [43]. In Australia, the reported rate in 2016 is even lower; only 10% of public Wi-Fi users said they use VPN [21]. Offering an automatic VPN connection service could increase its uptake. Google Fi[16] launched in late 2018 is an example. Subscribers' data are automatically encrypted through Google-run VPN server at all times[17].

A more promising solution is shifting the responsibilities from users to other stakeholders in the ecosystem: application developers, public Wi-Fi providers, and telecom providers. We should continue to encourage application developers to encrypt transmitted data. In light of the new EU General Data Protection Regulation (GDPR), failure to protect personal data of EU citizens could result in not only reputational damage but also potential fines of up to 4% of annual global turnover or €20 million (whichever is greater) [11] — sending a strong incentive to organizations to encrypt data. The tech industry could also help to play a role. Examples of initiatives already in place include: Microsoft using various encryption methods and protocols to protect data across its products such as Office 365 and Azure [22], Apple encouraging developers to encrypt data [7], and Google claiming to have designed security controls to reduce burden on Android developers [15].

[15] Defined by the applicable highest income tax rate. High-income and basic-income participants were subjected to 40% and 20% tax rate, respectively.

[16] https://fi.google.com/about/

[17] Only applies to mobile devices designed for Google Fi

For public Wi-Fi providers, there is currently no legal requirement in the UK that compels them to encrypt their network data by default. Businesses want customers to connect to Wi-Fi as easily as possible; hence, offering open unsecured Wi-Fi networks is a commercially attractive option. Policy makers could use the empirical evidence from our study to help to quantify the need to enforce encryption on all public Wi-Fi networks. The Japanese Ministry of Internal Affairs and Communications is discussing this possibility in preparation for the 2020 Tokyo Olympics [24]. In the near future, WPA3, a new standard of Wi-Fi security, may be a game-changer. It claims to offer an encryption mechanism without authentication [5]. Policy makers may consider promoting the benefits of WPA3 to encourage public Wi-Fi providers to implement it.

Government agencies responsible for cyber security could also consider working with telecoms regulators to review mobile data pricing and roaming charges. Allowing consumers to afford more data is similar to the *giving a bandwidth gift*, a concept which behavior economists view as a way to improve the quality of decision making among the poor whose minds were frequently taxed by financial constraints [25]. Cheaper plans would allow consumers to rely less on unsecured public Wi-Fi networks. The elimination of roaming charges within the EU states in 2017 showed that the share of travelers using mobile data roaming as often as in their home country had doubled in the first summer after the rule came into effect [12].

The insight about the effect of the resource preservation heuristic on decision-making and the tipping point it prompts users to take risks from using unsecured Wi-Fi networks could also be applied in a wider context in cyber security. Security interventions that do not sufficiently consider the resource preservation heuristic would fail in the same manner. We could use this insight to design more effective security interventions. For example, automatically activating security features and/or having them run in the background when the resources which users view as critical such as time and budget are running low, particularly at around 25-30%.

5.2 Limitations and possible future work

Our study has inherent limitations. First, we are aware of the possibility that participants may be cautious of using unsecured Wi-Fi after installing the app and change their habits. However, the three-month longitudinal study should be long enough to stabilize their routines. Some participants may not have connected to any unsecured Wi-Fi during the experiments because they were using less-regularly used devices to take part in the study or spend most of their time at their workplace and at home where there are secure Wi-Fi networks. There could also be unnoticed bugs that caused a failure in data collection. However, we considered this in our analysis as we included and excluded these participants which sufficiently addressed this limitation.

There are also uncommon threats to the external validity of our results — the behavior observed may not be universal among different profiles of participants. First, Android-based users may behave differently from non-Android users. Our samples were also restricted to UK residents. Mobile users in other countries, especially where mobile data is expensive or slow, could have different preferences. Future studies may seek to examine non-Android users and/or those outside the UK to confirm or contrast our findings. Moreover, our samples were drawn unequally among different demographics, some groups more than the others. But this is expected for studies using random selection for sampling. It is also possible that during the 3-month study, some participants may have traveled outside the UK; hence, being influenced to use unsecured public Wi-Fi to avoid financial penalties. However, considering our participants are residents of the UK, the probabilities of them traveling within EU states where there is no roaming charge is higher than traveling outside the EU. Future studies interested in replicating this study may consider tracking the geo-location of participants — though this may present an ethical challenge and therefore need to be designed carefully.

In addition, there could be other factors influencing the use of unsecured Wi-Fi networks which were not explored in this study e.g., the availability or connection speed of mobile data, how much participants value their data, etc. Future work could consider integrating these factors in the study and build a predictive model of how the users make a trade-off to further improve our understanding. Some of the statistically insignificant results from the correlation and causation analysis such as those reported on the effect of income and education level may reflect influences from underlying variables which future work could explore with a larger sample size to fully understand the causal factors. Future studies could also benefit from exploring people's perception of public Wi-Fi security at the point which traffic is decrypted at the router, instead of the security of the actual Wi-Fi link in this study. However, a high percentage of the general public is unlikely to be able to differentiate between the two types of risks, following similar user misconceptions about encryption highlighted in the literature [1, 32]; hence, the risks would need to be clearly explained to participants prior to the study. Finally, examining the effect of the resource preservation heuristic in a wider context of cyber security presents a research opportunity.

6 CONCLUSION

We examined factors influencing the use of unsecured Wi-Fi networks. The novelty in this study lies in the insight drawn from revealed preferences i.e., real life user-generated data collected through the *My Wi-Fi Choices* app. Our findings support the evidence from previous studies that examined stated preferences and showed that the constraint of mobile data brings about the resource preservation heuristic and significantly prompt users to use unsecured Wi-Fi. We also showed that not all types of resources instigates such behavior. While the level of remaining mobile data played a significant role, the remaining battery power played less of a role. Age, education, and income level also influence the decisions to use unsecured Wi-Fi networks.

Using unsecured networks is a worrying notion for policy makers keen to promote the security and privacy of online transactions. Since not everyone has unlimited mobile data, asking users to stop using such networks, especially when their mobile data allowances are running low, is ineffective. Encouraging users to use a protective tool (e.g., VPN) when making sensitive transactions on unsecured Wi-Fi networks could also help but the main challenge is convincing users to use these tools. We argue that a more promising solution is shifting the responsibilities to mitigate the risks to other stakeholders in the ecosystem: application developers, public Wi-Fi providers, and telecom providers.

REFERENCES

[1] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In *8th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 18)*.

[2] Action Fraud. 2016. Is public Wi-Fi as safe as you think? www.actionfraud.police.uk/news/is-public-wi-fi-as-safe-as-you-think-jan16

[3] Adhikari, Supratim. 2018. Free public Wi-Fi a consumer security risk. www.theaustralian.com.au/business/technology/free-public-wifi-a-consumer-security-risk/news-story/89482d2214873f9d3d2c19ddb013817f?nk=59fb9d61ba6176a68b04fde147c5600f-1521548822

[4] Marco Domenico Aime, Giorgio Calandriello, and Antonio Lioy. 2007. Dependability in wireless networks: Can we rely on WiFi? *IEEE Security & Privacy* 5, 1 (2007).

[5] Wi-Fi Alliance®. 2018. Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security.

[6] Atavina V Anastasia, Sergei V Zareshin, Irina S Rumyantseva, and Vitaliy G Ivanenko. 2017. Analysis of security of public access to Wi-Fi networks on moscow streets. In *Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian*. IEEE, 105–110.

[7] Apple. 2018. Developer Guide and Sample Code. https://developer.apple.com/library/content/documentation/General/Reference/InfoPlistKeyReference/Articles/CocoaKeys.html#//apple_ref/doc/uid/TP40009251-SW35

[8] Richard G Brody, Kyle Gonzales, and Dustin Oldham. 2013. Wi-fi hotspots: secure or ripe for fraud. *Journal of Forensic Investigative Accounting* 5, 2 (2013), 27–47.

[9] Ningning Cheng, Xinlei Oscar Wang, Wei Cheng, Prasant Mohapatra, and Aruna Seneviratne. 2013. Characterizing privacy leakage of public wifi networks for users on travel. In *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2769–2777.

[10] Conway, Richard. 2017. World Cup 2018: FA increases cyber security over hacking concerns. http://www.bbc.com/sport/football/41230542

[11] EU General Data Protectin Regulation. 2018. GDPR Key Changes. https://www.eugdpr.org/key-changes.html

[12] European Commission. 2017. The end of roaming charges within the EU. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2178

[13] F-Secure. 2014. The F-Secure Wi-Fi Experiment. www.fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f-secure.pdf

[14] Sascha Fahl, Marian Harbach, Thomas Muders, Lars Baumgärtner, Bernd Freisleben, and Matthew Smith. 2012. Why Eve and Mallory love Android: An analysis of Android SSL (in)security. In *CCS*.

[15] Google. 2018. Security. https://source.android.com/security/

[16] Junxian Huang, Feng Qian, Alexandre Gerber, Z Morley Mao, Subhabrata Sen, and Oliver Spatscheck. 2012. A close examination of performance and power characteristics of 4G LTE networks. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*. ACM, 225–238.

[17] iPass. 2018. Wi-Fi Growth Map. https://www.ipass.com/wifi-growth-map

[18] Benjamin D Kern. 2004. Whacking, joyriding and war-driving: Roaming use of Wi-Fi and the law. *Santa Clara Computer & High Tech. LJ* 21 (2004), 101.

[19] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. When i am on wi-fi, i am fearless: privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1993–2002.

[20] Anandi Mani, Sendhil Mullainathan, Eldar Shafir, and Jiaying Zhao. 2013. Poverty impedes cognitive function. *Science* 341, 6149 (2013), 976–980.

[21] Ian McShane, Mark A Gregory, and Christopher Wilson. 2016. Practicing Safe Public Wi-Fi: Assessing and Managing Data-Security Risks. (2016).

[22] Microsoft. 2018. Encryption. www.microsoft.com/en-us/trustcenter/security/encryption

[23] Miller A., Jen. 2016. The dangerous cost of free Wi-Fi. www.cio.com/article/3101859/wi-fi/the-dangerous-cost-of-free-wi-fi.html

[24] Ministry of Internal Affairs and Communications. 2016. Wireless-LAN Business Guidelines 2nd Edition. www.soumu.go.jp/main_content/000444788.pdf.

[25] Sendhil Mullainathan and Eldar Shafir. 2014. *Scarcity: the true cost of not having enough.* Penguin books.

[26] Munbodh, Emma. 2017. Why you should never use public wi-fi for online banking - and 5 other common mistakes. www.mirror.co.uk/money/you-should-never-use-public-10918012

[27] Munford, Monty. 2013. Lazy WiFi providers offer data-free risks for terrorists and criminals. www.telegraph.co.uk/technology/internet-security/10468317/Lazy-WiFi-providers-offer-data-free-risks-for-terrorists-and-criminals.html

[28] National Cyber Security Center. 2017. Keeping your smartphones (and tablets) safe. https://www.ncsc.gov.uk/guidance/keeping-your-smartphones-and-tablets-safe

[29] Norton Team. 2016. Public Wi-Fi security? Here's why you should use a VPN. https://uk.norton.com/norton-blog/2016/10/public_wi-fi_securit.html

[30] Ofcom. 2017. Adults' media use and attitudes - report 2017. https://www.ofcom.org.uk/__data/assets/pdf_file/.../adults-media-use-attitudes-2017.pdf

[31] Lucky Onwuzurike and Emiliano De Cristofaro. 2015. Danger is my middle name: experimenting with SSL vulnerabilities in Android apps. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 15.

[32] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. 2014. Why doesnâĂŹt Jane protect her privacy?. In *International Symposium on Privacy Enhancing Technologies Symposium*.

[33] Roberts, Gracie. 2016. Republican National Convention delegates unknowingly use fake Wi-Fi networks. https://blog.avast.com/republican-national-convention-delegates-unknowingly-use-fake-wi-fi-networks

[34] Jean-Marc Seigneur, Petra Kölndorfer, Marc Busch, and Christina Hochleitner. 2013. A survey of trust and risk metrics for a byod mobile working world. In *Third International Conference on Social Eco-Informatics*. 217–228.

[35] Anuj K Shah, Sendhil Mullainathan, and Eldar Shafir. 2012. Some consequences of having too little. *Science* 338, 6107 (2012), 682–685.

[36] Shaw, Nicholas. 2016. How Safe Is It To Connect To Public Wi-Fi Networks? www.huffingtonpost.co.uk/nicholas-shaw/how-safe-is-it-to-connect_1_b_12468328.html

[37] Tarek S Sobh. 2013. Wi-Fi networks security and accessing control. *International Journal of Computer Network and Information Security* 5, 7 (2013), 9.

[38] Nissy Sombatruang, Youki Kadobayashi, M Angela Sasse, Michelle Baddeley, and Daisuke Miyamoto. 2018. The continued risks of public Wi-Fi and why users keep using it: Evidence from Japan. In *In Press, 16th Annual Conference on Privacy, Security and Trust*. IEEE.

[39] Nissy Sombatruang, M Angela Sasse, and Michelle Baddeley. 2016. Why do people use unsecure public wi-fi?: an investigation of behaviour and factors driving decisions. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. ACM, 61–72.

[40] Dean Spears. 2011. Economic decision-making in poverty depletes behavioral control. *The BE Journal of Economic Analysis & Policy* 11, 1 (2011).

[41] Sulleyman, Aatif. 2017. Coffee shop Wi-Fi 'most dangerous' of all, warns security report. www.independent.co.uk/life-style/gadgets-and-tech/news/wifi-hotpots-coffee-shop-dangerous-security-risk-report-a7750091.html

[42] Colleen Swanson, Ruth Urner, and Edward Lank. 2010. Naïve security in a Wi-Fi world. In *IFIP International Conference on Trust Management*. Springer, 32–47.

[43] Symantec. 2017. Norton Wi-Fi Risk Report. www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf

[44] Christian Szongott, Michael Brenner, and Matthew Smith. 2015. METDS-A self-contained, context-based detection system for evil twin access points. In *International Conference on Financial Cryptography and Data Security*. Springer, 370–386.

[45] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of software updates: The process of updating software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 3215–3226.

[46] Kathleen D Vohs. 2013. The poor's poor mental power. *Science* 341, 6149 (2013), 969–970.

[47] Yu Xiao, Ramya Sri Kalyanaraman, and Antti Yla-Jaaski. 2008. Energy consumption of mobile youtube: Quantitative measurement and analysis. In *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on*. IEEE, 61–69.

A SURVEY QUESTIONS

1. What is your gender?

- Male
- Female
- Prefer not to say

2. What is your age group?

- Under 18
- 18-25
- 26-35
- 36-65
- 65+

3. What is the highest level of education you have completed?

- Some high school
- High school graduate
- Diploma/Vocation training
- Bachelor's degree
- Postgraduate's degree

4. What is your current employment status? Please choose one that best describes your status.

- Full time students
- In part-time employments
- In full-time employments
- Not working
- Retired

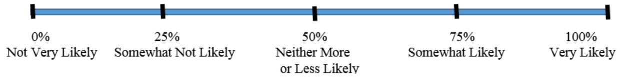
5. What is your income level? Please choose one UK income tax rate that best describes it.

- Personal allowance (0%): Less than £11,000
- Basic rate (20%): £11,000 to £43,000
- Higher rate (40%): £43,001 to £150,000

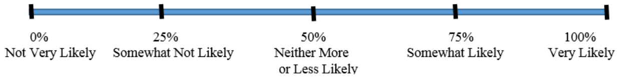
6. In the past year, have you or any person close to you ever fallen victim of online-related fraud (e.g. accounts hacked or data breached)?

- Yes
- No

7. From your perspective, what is the likelihood that security could be compromised when using mobile data plan to connect to the Internet?



8. From your perspective, what is the likelihood that security could be compromised when using free public Wi-Fi to connect to the Internet?



B DEMOGRAPHY OF PARTICIPANTS

Table 2: Demography of all participants

Gender	n	%	**Income Level (by Income Tax Rate)**	n	%
Female	42	59.15	Personal allowance (0%): Less than £11,000	31	43.66
Male	29	40.85	Basic rate (20%): £11,000 to £43,000	31	43.66
Total	71	100.00	Higher rate (40%): £43,001 to £150,000	9	12.68
			Total	71	100.00
Age	n	%	**Employment**	n	%
18-25	34	47.89	Full time students	30	42.25
26-35	25	35.21	In full-time employments	28	39.44
36-65	12	16.90	In part-time employments	7	9.86
Total	71	100.00	Not working (but not on retirement)	4	5.63
			Retired	2	2.82
			Total	71	100.00
Education Level	n	%			
Some high school	3	4.23			
High school graduate	9	12.68			
Diploma/Vocation training	6	8.45			
Bachelor's degree	29	40.85			
Postgraduate's degree	24	33.80			
Total	71	100.00			