Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions

Nissy Sombatruang
Department of Security and Crime Science
+44 (0)20 3108 3046
uctznso@ucl.ac.uk

M. Angela Sasse
Department of Computer Science
+44 (0)20 7679 7212
a.sasse@ucl.ac.uk

Michelle Baddeley
Bartlett School of Construction and Project Management
+44 (0)20 3108 3218
m.baddeley@ucl.ac.uk

University College London, Gower St, London WC1E 6BT, UK

ABSTRACT
Public Wi-Fi networks are now widely available in many countries. Though undoubtedly convenient, such networks have potential security and privacy risks. The aim of this study was to understand if people are aware of those risks, and – if so – why they decide to take them. We set up an experimental free Wi-Fi network at 14 locations in central London, UK, for a period of 150 hours, and people connected most often to use instant messaging, search engines, and social networks, and sensitive data (such as name, date of birth, and sexual orientation) were transmitted. We subsequently investigated people's risk awareness and risk behaviour through semi-structured interviews with 14 participants, and an online scenario-based survey with 102 participants. The majority of participants said they would use public Wi-Fi under circumstances where the risks taken are not consistent with maximising utility. Female participants rated the risks associated with public Wi-Fi use, more highly – and yet more females than males said they would use them to save their data plans. These findings align with insights from behavioural economics, specifically the insight that people can misjudge risky situations and do not make decisions consistent with expected utility theory.

CCS Concepts
• Security and privacy → Network security → Mobile and wireless security • Security and privacy → Human and societal aspects of security and privacy → Privacy protections

Keywords
Public Wi-Fi Security, People and Security, Data Leakage

1. INTRODUCTION
Public Wi-Fi networks have become ubiquitous in urban areas over the past decade, offered in high-traffic areas such as transport hubs, coffee shops, or near popular tourist attractions. Many of these public Wi-Fi networks are open and free to use, and do not require users to authenticate. But as a number of previous studies have shown, most of these networks are unsecured, so when connecting users expose themselves – knowingly or unknowingly - to security and privacy risks.

We investigated people's connection behaviour and perceptions of associated risks and benefits around three questions: 1. How often will people connect to an insecure public Wi-Fi network, in a busy city centre (London, UK)? 2. Do they expose sensitive information when using those networks?, and 3. How do people reason about the costs and benefits associated with public Wi-Fi use? The last question is particularly intriguing as mainstream economic theories – specifically expected utility theory, argues that people make decisions rationally using mathematical decision-making rules whilst behavioural economics has demonstrated extensive evidence of bounds to rationality consistent with people misjudging risky situations – a theme developed in the context of prospect theory and other behavioural theories of risky decision-making.

We conducted our study into three parts. First, we examined how often and for what purpose, people will connect to public Wi-Fi networks. We set up our own open public Wi-Fi network at 14 public locations in central London, for a total of 150 hours. The second part of the study investigates security and privacy implications. We inspected the data packets to see if sensitive information was transmitted insecurely. We found applications and websites leaking cookies that contained personal information and online transaction history.

In the third part of our study, we elicit the reasons why people use public Wi-Fi. We interviewed 14 participants to gain preliminary understanding of their rationales and used the result to design questions in the subsequent scenario-based online survey. We conducted this survey with 102 participants to determine if their decisions to connect to public Wi-Fi can be explained in terms of expected utility. We found that a significant proportion of our participants did not make choices predicted by utility theory and instead were consistent with insights from behavioural economics, specifically the argument that people do misjudge risky situations and do not make decision mathematically as proposed in the utility theory. We also found a correlation with gender, employment status, and perceived security of pubic Wi-Fi.

The paper is structured as follows: Section 2 provides related work, and Section 3 introduces the methodology. We present the results in Section 4 and discuss the application of our findings in Section 5, before presenting the conclusion in Section 6.

STAST '16, December 05-05, 2016, Los Angeles, CA, USA

ACM ISBN 978-1-4503-4826-3/16/12.
http://dx.doi.org/10.1145/3046055.3046058

2. RELATED WORK

Wireless networks provide a convenient way for people to connect to the Internet, and many businesses see it as beneficial to offer free Wi-Fi [15]. In the UK, there are now approximately 269,000 free Wi-Fi hotspots [14], and more than 200 underground stations in London now provide free Wi-Fi [44] – which for instance helps people to work out alternative travel in case of disruptions. However, there are security risks to using a public Wi-Fi network. In this section, we explore the relevant literature of the extent of public Wi-Fi usage, the security and privacy implication of using such networks, and the decision making process for using public Wi-Fi network. Each is discussed in turn.

2.1 Extent of public Wi-Fi usage

A number of studies report people use public Wi-Fi to perform a range of online activities. A study of public Wi-Fi usage in Australia [29] noted that people used public Wi-Fi for interpersonal support, emails and social media such as Facebook to communicate with friends and family - but also to 'kill time' by surfing the Internet. A study in Seattle and Boston [20] found that people use public Wi-Fi for email and for instant messaging their friends and families. However, both studies collected self-reported behaviour (survey and interviews) rather than observed behaviour.

In 2012, Hare et al. [23] set up an experimental Wi-Fi network on public transit buses in the northern Midwest of the US, and found users mainly use the network to access entertainment content. In a similar experiment at the ACM conference in San Diego in 2002 [5], 195 distinct devices connected to the researchers' Wi-Fi networks and more than 50% of generated traffic was Web and SSH traffic. Another study by Cheng et al. conducted at 15 airports across the US, Germany, Australia, and India [12] reports that people used unsecure public Wi-Fi at the airports for online shopping and social networking. A study conducted in Canada [34] showed that cafés are the most popular spots for unsecured public Wi-Fi connection. A study in Nottingham in 2014 [35] found that users use the experimental public Wi-Fi networks to access entertainment content. The study took place in Aspley - a medium sized British city with a population of around 300,000.

Many people in the UK now have data plans, and so do not have to rely on unsecured public networks to access the services that people were found to use in previous studies. Does this mean public Wi-Fi is used less? The continuing increase in the number being offered suggests there still is demand.

Hence, our first hypothesis;

H_1: People connect to public Wi-Fi and use them for a range of purposes.

2.2 Security and privacy implications of using public Wi-Fi

A malicious user can intercept data sent over unsecured public Wi-Fi [26]. In the UK, the City of London Police warned that criminals use public Wi-Fi to intercept credit card details by setting up evil twin (spoof) networks or Man-in-the-middle (MITM) attacks [14] – this has also been reported elsewhere ([3], [7], [33],[37] [39]).

The broadcast nature of public Wi-Fi also increases the risk of data being intercepted and potentially read by anyone within the range of the Wi-Fi network [28]. A large-scale study conducted at 15 airports across the US, Germany, Australia, and India [12] discovered that two thirds of users leak private information such as pictures of merchandise that a user had previously browsed and social groups of interest whilst accessing the Internet at the airport. Another study by Chen et al. [11] found sensitive information such as medical history, family income, and investment secrets leaking from a Wi-Fi side channel. A study conducted at two locations in London on behalf of F-Secure [15], found one username and password being visible as they pass through the experimental Wi-Fi hotspot. However, the second experiment lasted for only 30 minutes which is a relatively small window to fully draw a conclusion on. We wanted to conduct a similar experiment in our study, but over a longer time period.

Based on the findings from previous studies and news reported, we hypothesise that security and privacy of data can be compromised whilst being transmitted on public Wi-Fi.

Hence, our second hypothesis;

H_2: Security and privacy of data can be compromised on public Wi-Fi network.

2.3 Reasons for using public Wi-Fi

Many people use public Wi-Fi because it offers them utility. Swanson et al. [38] found that - although users were aware of certain risks - they often do not believe the risk will be realised. Their study used a qualitative approach. We wanted to check the awareness of security risks in a more systematic way. Klasnja et al. [28] suggested that public Wi-Fi users believe the security measures on their devices will protect them, but their study did not explain the decision-making process for such behaviour. Ferreira et al. [16] investigated the effects of trust and context when choosing public Wi-Fi network's names and found that adding security or freeness in the network's names does not bias user's preference in familiar environments, but the opposite behaviour was observed in unfamiliar contexts. Ferreira et al. [17] also examined whether the graphical cues (specifically, a security padlock and signal strength bars) convey their intended messages in informing users of the security of a given public Wi-Fi network. They found that participants' understanding of the cues and the circumstances are the real motivators behind the participants' choices.

Studies that investigate the decision-making process that leads people to connect to public Wi-Fi are limited. Ferreira et al. [18] used the UML sequence diagram to explain the steps that the user undertakes when connecting to public Wi-Fi networks. However, their models focused on pay-per-use hotspots and Internet Service Provider (ISP)'s homespot (i.e. a residential router provided by the ISP that makes available part of its capacity to other customers who may be within range of the Wi-Fi network), and did not include scenarios for users connecting to free public Wi-Fi and other Wi-Fi networks that do not require registration, and which are widely offered in the UK. We addressed these elements in our study.

Jeske et al. [22] investigated factors that drive participants to choose one Wi-Fi network over others, and found that the absence or presence of the 'padlock' icon drove decision-making. This study assumed that participants are committed to connect to public Wi-Fi, and have no alternative (such as using mobile data). Our study addresses a different goal: we wanted to understand the process people go through, and the factors they consider in their decision to connect - or not - to a potentially unsecure Wi-Fi network when a more secure alternative is available. Yevseyeva et al. [47] proposed a model of the trade-offs involved in choosing between different Wi-Fi networks, but their model is not supported

by empirical evidence. We wanted to better explain people's decision making processes by using empirical evidence.

There are general decision-making theories and frameworks that can be applied to understand why people use public Wi-Fi and accept the associated risks. One of them is the expected utility theory proposed by Von Neumann and Morgenstern [46] which is used widely in the game and economic behaviour literature and [36] is arguably the major paradigm in decision-making since World War II. It is a theory which [6] predicts a person's choice, and [32] is particularly suited to analysing choice among risky alternatives. According to utility theory [6], people's decisions are made to ensure that they maximise their expected utility. In the context of our study, it means that people decide to connect - or not - to public Wi-Fi networks to maximise expected utility (EUT) – i.e. they would want to catch up with work, or chores such as paying bills, and consume entertainment content when it is safe to do so. At the same time, we would not expect them to risk exposing credentials or private data.

Hence, we formulated our 3rd hypothesis in line with expected utility theory.

H_3: People choose action that gives the highest expected utility, when deciding to connect, or not to connect, to public Wi-Fi.

Our alternative hypothesis in this case, consistent with behavioural economics, is that people's decisions around risk may systematically deviate from EUT.

In this section, we present the related work. The next section, Section 3, discusses the methodology.

3. METHODOLOGY

Our study consists of three main parts. The first part investigates the extent of public Wi-Fi usage and the second part examines the security and privacy risks from using public Wi-Fi networks. The final part concerns examining people's rationale for using public Wi-Fi and bearing the risks of data being compromised. The methodology for each part of the study is discussed in this section.

3.1 The extent of public Wi-Fi usage

The objectives of this part are to verify if people do connect to public Wi-Fi networks and, if so, to explore the nature of Internet transactions they perform. We setup a free open public Wi-Fi network at various locations in London and monitored the Wi-Fi traffic. The following sub sections explain the setup of the experimental Wi-Fi network.

3.1.1 Setting up an experimental public Wi-Fi

Our experimental Wi-Fi hotspot consisted of an Acer Windows 7 operating system laptop, an iPad Air 2 Cellular (version 9.3.2), an O2 data sim card, a USB cable (for connecting an iPad to a laptop), Apple iTunes (version 12.3.3.17), and ARP Miner software (version 2.2.3). Apple iTunes provided a network driver that allows the laptop and the iPad to communicate and share the Internet connection. We used the ARP Miner software to create a captive portal, a login page which forces a user to accept the terms and conditions of usage before using our Wi-Fi network. This step is critical to meet the UCL Ethics Committee (IRB) requirement that we must obtain consent from every participant who tries to connect to the network (see 3.1.5 for ethics approval).

To set up the experimental Wi-Fi network, we first inserted the O2 data sim card into the iPad. Then we used the iPad's built-in "Personal Hotspot" function to share the Internet connection with the Windows 7 laptop via a USB cable. Next, on our Windows 7 laptop, we used the "Internet Connection Sharing" function to create an open Wi-Fi network called "Free London Wi-Fi" and use it as our experimental Wi-Fi network (Figure 1).

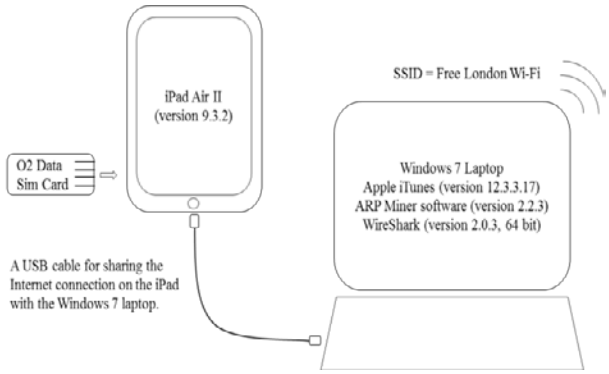

Figure 1. Components of the experimental free public Wi-Fi in this study.

3.1.2 Monitoring Wi-Fi traffic

We enabled the authentication log in the ARP Miner software to capture the Media Access Control (MAC) address of the participants' device. This helped us to identify a unique number of devices connecting to our experimental Wi-Fi network. To monitor the Internet traffic, we installed WireShark (version 2.0.3, 64 bit), a network protocol analyser, on the Windows 7 laptop. After the participants had accepted the terms and conditions, traffic routing from the participants' devices to the Internet via our experimental Wi-Fi network were captured by WireShark.

3.1.3 Locations and duration of the experiment

We set up our experimental open free public Wi-Fi network at various locations and times in central London. Since there is only one set of equipment, the experiment took place at one location at a time. Various types of locations, for example, train stations and popular tourist locations, were chosen to allow us to observe any potential differences in participants´ behaviour when they were using public Wi-Fi networks. The experiment was run for a total of 150 hours over a period of one and a half months between May and June 2016. A summary of locations where the experiment took place and the hours of each experiment is in Table 1.

Table 1. Locations and hours of the experiment

Type of Location	Location	Hours of experiment
Transport	Waterloo Train Station	20
	Victoria - Bus Station	15
	King Cross Train Station	10
Leisure	Fulham Broadway Centre	15
	Leicester Square	15
	South Kensington	8
	South Bank	8
	Piccadilly Circus	6
	Tower of London	5
Park	Hyde Park	10
	St. James Park	8
	Regent Park	5
Educational	British Library	20
	UCL Campus	5
Total		150

3.1.4 Analysing the result

We identified a unique number of devices connecting to our experimental Wi-Fi networks by using the MAC address. We

differentiated the MAC addresses of devices attempting to connect to from the MAC address of those devices connected successfully (i.e. devices which the owners had accepted the terms and conditions of using our experimental Wi-Fi network) by segregating entries in the log that contain "Client Entries" and "Client Authorized" in the description field, respectively. We focused our analysis on the devices in the latter group as they were able to connect to the Internet.

We used Microsoft Excel to sanitise and analyse traffic captured by WireShark. Since our goal was to examine the transactions that participants carried out when connected to our experimental Wi-Fi, data cleansing was critical to filter out, as far as possible, any irrelevant Internet traffic from the raw data. Irrelevant traffic included background traffic that was not directly initiated by users (such as captive portal traffic, routine broadcasting messages from the router to devices within the Wi-Fi network, operating system updates, background advertising or web analytics traffic, and potential malware traffic, if users' devices were infected). Since there is no single source of information which lists all possible non-user initiated traffic, we used a combination of sources such as Google Search Engine, Google Scholar, Wikipedia, mobile phone forums, and WireShark to help us identify these background jobs.

Next, to identify potential websites or the applications used, we examined traffic entries classified as Domain Name System (DNS) protocol. As an example, a DNS entry which contains "Standard query 0x9870 A e11.whatsapp.net" in the info field indicates that a participant is using WhatsApp, a messaging application. Since there is no official database that can identify all DNS traffic and their corresponding websites or applications, and not all types of DNS traffic are publicly well-known, we used the Google search engine and other Internet sources discussed above to help us identify and verify the websites and the applications.

3.1.5 Ethics Approval

We submitted the study design to UCL's Research Ethics Committee (IRB) prior to starting the fieldwork. Permission was granted provided participants accepted the Terms and Conditions, which explained that they would be connecting to the Internet using a captive portal technology. Participants had to agree that data such as IP address, MAC address, and network traffic would be collected. The data we collected were stored in an encrypted drive accessible only to the research team.

3.2 Security and privacy risk of using public Wi-Fi

To identify potential security and privacy risk from using public Wi-Fi networks, we inspected Internet packets passing through our experimental Wi-Fi network which were captured by WireShark. In particular, we searched for packets that contain sensitive information such as passwords, cookies, and packets that travelling through port 80, a standard port for unencrypted http traffic[1].

We also examined packets that travel through well-known email protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP), as they could reveal the content of the emails if not configured correctly.

[1] www.en.wikipedia.org/wiki/Port_80

3.3 Reasons for using public Wi-Fi

We adopted both qualitative and quantitative approaches to examine people's rationale for connecting to unsecured public Wi-Fi network. Each method is discussed in turn.

3.3.1 Qualitative study – user interview

The main purposes of the interview are to understand participant's rationales for using unsecure public Wi-Fi and to use the result to inform the design of the subsequent quantitative online survey.

We advertised our study via flyers at various locations on the UCL campus, the Monthly UCL Student Newsletter (May 2016), the Department of Security and Crime Science (SCS) Twitter account, the Department of SCS MSc student mailing list, and London VISION Singers group. Interested participants were asked to fill out an online pre-screening questionnaire which allowed us to assemble a demographically balanced sample of participants.

We interviewed 14 participants chosen from a range of demographic groups (Table 2). We gave information sheet to participant and obtain user consent prior to the interview. Each participant received £10 for a one-hour interview.

Table 2. Demographic of participants in the interview

Main category	Subcategory	No. of participants
Gender	Male	7
	Female	7
Age	18-24	5
	25-34	3
	35-44	2
	45-54	1
	55-64	1
	65-74	1
	Prefer not to say	1
Education	High School	3
	Diploma Training	1
	Bachelor's Degree	5
	Postgraduate Degree	5
Usage of Internet via public Wi-Fi	Always	3
	Nearly daily	3
	> a few (2-3) times/week	2
	< a few (2-3) times/week	6

During the interview, we asked participants about their general perception and experience of using open public Wi-Fi networks, their perception of risks and security of public Wi-Fi, and their rationale when deciding to connect, or not to connect, to unsecure public Wi-Fi. We audio-recorded and transcribed each interview session. We then coded the interview response based on a defined group of categories designing to help us understand participants' behaviour and rationale for using unsecured public Wi-Fi networks.

3.3.2 Quantitative study - online survey

We used a scenario-based online survey to examine a participant's rationale when they decide to connect, or not to connect, to unsecure public Wi-Fi networks. We designed the survey questions to test our main research hypothesis that participants would choose the action that yields the highest expected utility. We created eight fictitious scenarios in which Internet access would be beneficial and - for each scenario - asked the participant to choose among three choices: a) connect to the Internet via a mobile data plan or

data roaming, b) connect to the Internet via an open public Wi-Fi network, or c) not connect to the Internet.

The eight fictitious scenarios cover different locations, types of transactions, degree of urgency (see Table 3). Within each scenario, there are four sub-scenarios where participants have 100%, 75%, 50%, and 25% left on their mobile data plans or roaming. The survey also asked participants some general demographic questions, usage of the Internet, and perception of security risk and general risks. This is to allow us to subsequently evaluate correlation between these factors and their behaviour when using public Wi-Fi.

Table 3. Cases by transaction type, urgency, and location

Case	Type of Transaction	Urgency	Location
I	Non-financial	Non-urgent	In the UK
II	Non-financial	Urgent	In the UK
III	Financial	Non-urgent	In the UK
IV	Financial	Urgent	In the UK
V	Non-financial	Non-urgent	Outside the UK
VI	Non-financial	Urgent	Outside the UK
VII	Financial	Non-urgent	Outside the UK
VIII	Financial	Urgent	Outside the UK

Expected utility is unobservable so we have assumed that expected utility will be a function of expected value. To enable us to calculate the expected value of each choice and subsequently compare whether the choice that the participants selected yields the highest utility per our hypothesis, our questions were designed to elicit the value of each variable, per generic expected value (EV) equation (See (1)) based on model proposed by Von Neumann and Morgenstern [46].

$$EV = p_1(v_1-c_1) + p_2(v_2-c_2) + \ldots + p_i(v_i-c_i) \quad (1)$$

Where p is the probability of success for each choice, v is the expected value received if success, c is the cost associated with each choice, and i is the set of all possible outcomes.

Applying the equation to our study, we have equations (1.1), (1.2), and (1.3) for the expected value of using public Wi-Fi (EV_w), mobile data plan (EV_m), and not connecting to the Internet at all (EV_n), respectively.

$$EV_w = p_w(v_w-c_w) + p_{ws}(v_{ws}-c_{ws}) + p_{wis}(v_{wis}-c_{wis}) \quad (1.1)$$

Where p_w is the probability of connecting to the Internet via public Wi-Fi is successful which we assume it to be 1, v_w is the participant's expected value from connecting to the Internet, c_w is the cost of free public Wi-Fi which we assume to be 0, p_{ws} is the participant's perceived likelihood that data travel securely on public Wi-Fi (i.e. 1-p_{wis}), v_{ws} is the participant's expected value from connecting to the Internet securely, c_{ws} is the cost of acquiring secure connection which we assume it to be 0 (for simplicity of the model, secure connection is offered as free in all scenarios), p_{wis} is the participant's perceived likelihood that data can be compromised on public Wi-Fi, v_{wis} is the participant's expected value if data is compromised, and c_{wis} is the cost of acquiring an insecure connection which is 0 (i.e. we assume that open public Wi-Fi is insecure so participant pays nothing for not connecting to secure service).

$$EV_m = p_m(v_m-c_m) + p_{ms}(v_{ms}-c_{ms}) + p_{mis}(v_{mis}-c_{mis}) \quad (1.2)$$

Where p_m is the probability of connecting to the Internet via mobile data is successful which we assume to be 1, v_m is the participant's expected value of connecting to the Internet, c_m is the cost of using a mobile data plan, p_{ms} is the participant's perceived likelihood that data travels securely on the mobile data network (i.e. 1-p_{mis}), v_{ms} is the participant's expected value of connecting to the Internet securely, c_{ms} is the cost of acquiring a secure connection which we assume to be 0 (for simplicity of the model, secure connection is offered as free in all scenarios), p_{mis} is the participant's perceived likelihood that data can be compromised on mobile data network, v_{mis} is the participant's expected value if data is compromised, and c_{mis} is the cost of acquiring insecure connection which is 0 (i.e. we assume that open public Wi-Fi is insecure so the participant pays nothing for acquiring insecurity).

$$EV_n = p_n(v_n-c_n) \quad (1.3)$$

Where p_n is the probability of not connecting to the Internet (which is always 1 as the participant has decided not to connect to the Internet), v_n is the participant's perceived utility of not connecting to the Internet, and c_n is the cost of not connecting to the internet which is 0.

For variables used to measure expected values (i.e. variable 'v' in (1.1), (1.2), and (1.3)), we designed the questions based on the concept of "Willingness to Pay (WTP)" and "Willingness to Accept (WTA)". This concept is used widely in an economic analysis to derive empirical estimates of welfare measures [1]. In our study, the WTP refers to the maximum amount that the participant is willing to pay for an Internet connection, and for a secure Internet connection. The WTA, on the other hand, refers to the amount that an individual is willing to accept in exchange for giving up an Internet connection, and for a secure Internet connection, respectively. An example of case description and questions from scenario I are in Appendix A.

A total of 106 participants were recruited via Prolific Academic (PA). We restricted our eligible participants to only those older than 18, currently living in the UK, and have a PA approval rate of no lower than 90%. Survey responses were refined to optimise data quality. Records that do not contain all required fields that have the same values for every variable were removed. We also removed a survey that failed both of our fatigue tests. After data cleansing, we have 102 responses from various demographic groups (Table 4).

Table 4. Demographic of online survey participants

Main category	Subcategory	No. of participants
Gender	Male	42
	Female	60
Age	18-24	16
	25-34	31
	35-44	26
	45-54	17
	55-64	10
	65-74	2
Education	Bachelor degree	43
	Completed high school	6
	Diploma	12
	High school graduate	25
	Postgraduate degree	16
Employment Status	Doing something else	9
	Full-time education	15
	Fully retired from work	5
	Unemployed	8
	In full-time employment	50
	In part-time employment	15

We used Survey Gizmo (www.surveygizmo.com) to create the online survey. To optimise data quality, we embedded rules such

as rejecting negative values for WTP and WTA. Moreover, we used a simple interface (sliding bar) to allow participants to choose a value between 0% and 100%. All participants were given the same eight scenarios. However, to minimise the anchoring effect and response bias, the order of the eight scenarios was selected randomly.

For each participant and for each scenario, we calculated the expected value of each of the three choices given to the participant and determined if the participant had selected the choice that yields the highest expected value according to our hypothesis. Finally, we performed a binomial test and a binomial logistic regression using SPSS. We used binomial test (See (2)) to determine whether a proportion from a single dichotomous variable is equal to a presumed population value. In our study, it is to test whether 100% of our participants acts according to the utility theory per our hypothesis and, if not, whether the differences observed is statistically significant.

$$Z = \frac{p_1 - p_0}{\sqrt{p(1-p)(1/n_1+1/n_2)}} \quad (2)$$

Where p_1 is the actual proportion of participants who act in accordance with the utility theory when deciding to connect (or not) to public Wi-Fi, p_0 is the hypothetical proportion of participants (in our study, this is 100% per the hypothesis), p is the proportion of successes for the combined sample, n_1 is the number of participants making a decision in line with the utility theory, and n_2 is the number of participants whose actions do not align with the theory.

We also used a binomial logistic regression analysis (See (3)) to assess the effects of independent variables (e.g. demographic variables), on participants' decision making when it comes to deciding to connect, or not to connect, to unsecure public Wi-Fi.

$$\pi_i = Pr(Y_i=1|X_i=x_i) = \exp(\beta_0+\beta_1 x_i)/1+\exp(\beta_0+\beta_1 x_i) \quad (3)$$

Where Y is a binary response variable, $Y_i = 1$ if participant make a decision in line with utility theory, $Y_i = 0$ if participant do not make a decision in line with the theory, $X = (X_1, X_2, \ldots, X_k)$ is the independent variables (e.g. age, gender, average use of online communication, etc.).

Finally, we analysed the Nagelkerke R^2 value to determine the percentage of variation in the dependent variables that is explained by the model.

In this section, we discussed the methodology used in our study. The next section, Section 4, discusses the analysis of the results.

4. ANALYSIS OF RESULTS

The following sections discussed the detailed results from each part of the study.

4.1 Extent of public Wi-Fi usage

We found evidence of participants connecting to our Wi-Fi for a variety of purposes.

4.1.1 Result by location

Participants connected to our experimental Wi-Fi at various locations. Overall, one device attempts to connect to our experimental Wi-Fi every two hours (0.43 device/hour), and one device connected successfully and used the Internet every four hours (0.23 device/hour). The rates of device connecting vary by location (Table 5). We did not observed any successful connections at UCL Campus, Fulham Broadway, Leicester Square, South Kensington, St. James Park, and Regent Park.

However, we intentionally did not design these figures to be statistically comparable because our research question focuses on investigating whether people would connect to public Wi-Fi rather than statistically testing the differences in the extent among diverse locations. The latter would require a different research design which includes, for examples, classifying peak vs. non-peak time, and statistically testing the differences in mean among locations.

Table 5. Connected devices by location

Location	No. of hours	Devices attempting to connect (per hour)	Devices connected successfully (per hour)
Victoria Bus Station	15	1.07	0.73
Tower of London	5	1.00	0.60
Waterloo Station	20	1.00	0.60
South Bank	8	0.38	0.25
King Cross Station	10	0.50	0.20
Piccadilly Circus	6	0.17	0.17
British Library	20	0.25	0.10
Hyde Park	10	0.10	0.10
UCL Campus	5	0.00	0.00
Fulham Broadway	15	0.07	0.00
Leicester Square	15	0.20	0.00
South Kensington	8	0.13	0.00
St. James Park	8	0.38	0.00
Regent Park	5	0.00	0.00
Total	150	0.43	0.23

4.1.2 Result by nature of transactions

We found that participants carried out a range of activities whilst connecting to our experimental Wi-Fi. *Google Search Engine*, *Facebook*, *Apple iTunes*, *WhatsApp*, *SnapChat*, and *Instagram* are the most popular, accounting for nearly half of the total usage. We observed traffic to websites outside the UK (e.g. *UOL Mail Brazil*, *Observador News Portugal*, etc.) which indicate that participants connecting to our Wi-Fi network may be from overseas. Within the top ten most used websites/apps, we found traffic that we were unable to identify. They could be traffic from malware that were not well-known or traffic from private company not listed publicly on the Internet. Table 6 shows a list of the top ten websites/apps.

Table 6. Top ten websites/application observed

Web/App Category	Sessions	Web/App Category	Sessions
Google Search	34	Instagram	7
Facebook	20	Unknown	6
Apple iTunes	18	Google Mail	6
WhatsApp	13	Potential Malware	5
SnapChat	7	Apple Facetime	5
Total	121		

4.2 Security and privacy risk of using public Wi-Fi network

We found no evidence of usernames and passwords being transmitted in the clear. However, we observed six applications/websites that leaked cookies that could compromise data privacy. These apps/webs include *Instagram* (Social Network), *Yelp* (Miscellaneous), *Channel 4* (TV), *Betfair* (Online

Gambling), *Bumble* (Online Dating), and *Desperaco* (Online News).

The cookies from *Instagram* contain URL links to MP4 videos, which participants were watching whilst using our experimental Wi-Fi network. We were able to replay these videos by copying and pasting the links to a web browser. Similarly, in the cookies from TV station *Channel 4* we extracted a list of TV shows viewed by participants. The cookies from *Yelp* and *Desperaco* contained links to the photos viewed by participants. For *Betfair*, the cookies contained data that could potentially be part of betting transactions.

The cookies leaked from *Bumble*, an online dating application used by approximately 800,000 users as of August 2015 [31], contained private information and online dating history. We observed not only the profile information of the individual connecting to our experimental public Wi-Fi network, but also 29 other profiles that the individual had viewed. These profiles included information such as name, date of birth, photo, education, and sexual orientation, and, in some cases, an Instagram username which allows us to find out more information about him/her. We also noted that even though the URL links to profiles photo were configured as "https", we could replace it with "http" in a web browser and view these photos without having to sign up or install Bumble application. An example of the cookie from *Bumble* is in Figure 2 with sensitive information redacted.

Figure 2. An example of unencrypted sensitive information being sent from Bumble app.

4.3 Reasons for using public Wi-Fi

We discussed the results from both the quantitative and the qualitative studies in this section.

4.3.1 Results from interviews

More than 90% of our participants expressed concerns about public Wi-Fi security, and, among those, more than 50% of participants use public Wi-Fi networks regardless, despite being aware of the risk. However, when asked about the rationale for their behaviour, the responses varied.

The most common reason given is that it is free. For example, Participant No. 5 (P5) said "*When we were in Australia, it [the Wi-Fi] was £10/hour and we found that by going to a post office there are [free] Wi-Fi hotspots and we told everyone to go to [the] Wi-Fi hotspots. Again, that's probably not secure but it's [better] than paying for Wi-Fi at the hotel*". P13 also shared a similar rationale "*Sometimes, on Wi-Fi, you are afraid that data transfer might not be safe. You have no control who is receiving on the other side. But well, it's free*".

However, some participants could not precisely explain their rationale. For instances, P8 explained, "*It's weird 'cos I know it can happen that people can track you [when you use public Wi-Fi] but still I connect to it*". P5 also explained her rationale as "*It [public Wi-Fi security] is in the back of my mind but I don't consciously [think about it]…if I want to access it [public Wi-Fi], I access it*". P2 said that "*At the time, I just don't think about it. I just think about I want to use the Wi-Fi*".

4.3.2 Result from online survey

Regardless of the urgency and the nature of transactions and the location where the scenario takes place, we found that, in most cases, a large proportion of participants consistently do not make choices as predicted by the expected utility theory when deciding to connect (or not) to public Wi-Fi and these results are statistically significant.

For general non-urgent non-financial transactions (case I) and urgent non-financial transactions (case II) where the scenario located the user in the UK, we observed that participants choose the option that gives them highest expected value in urgent situations when they still have 100% and 75% left of their mobile data plan. The reverse behaviour was observed when they had 50% and 25% left.

When the scenario located the user outside the UK (case V for non-urgent and case VI for urgent non-financial transactions), however, participants consistently do not choose the option that gives them highest expected value regardless of how much roaming mobile data they have left. In each scenario, the binomial test showed that the proportion of participants who make choices per the utility theory significantly deviates ($p < 0.001$) from the presumed population value of 100% (Table 7 and 8).

Therefore, overall, there is sufficient evidence to reject the claim that people choose action that gives the highest expected value, when deciding to connect, or not to connect, to public Wi-Fi, particularly for making general non-financial transactions.

Table 7. Binomial test results for non-urgent transactions

Data plan level	Group*	Case I UK		Case V Outside UK	
		N	Observed Prop.**	N	Observed Prop.**
100%	1	31	0.30	44	0.43
	2	71	0.70	58	0.57
75%	1	32	0.31	45	0.44
	2	70	0.69	57	0.56
50%	1	38	0.37	47	0.46
	2	64	0.63	55	0.54
25%	1	48	0.47	52	0.51
	2	54	0.53	50	0.49

Table 8. Binomial test results for urgent transactions

Data plan level	Group*	Case II UK		Case VI Outside UK	
		N	Observed Prop.**	N	Observed Prop.**
100%	1	33	0.32	36	0.35
	2	69	0.68	66	0.65
75%	1	33	0.32	32	0.31
	2	69	0.68	70	0.69
50%	1	37	0.36	35	0.34
	2	65	0.64	67	0.66
25%	1	37	0.36	42	0.41
	2	65	0.64	60	0.59

[*]Group 1 is a group of participants making choice according to the utility theory, Group 2 is a group of participants not making choice according to the theory.[**]All result significant at $p < 0.001$.

For financial transactions (Case III-non urgent in the UK, Case IV-urgent in the UK, Case VII-non-urgent outside the UK, and Case VIII-urgent outside the UK), a statistically significant proportion of participants consistently make choices not predicted by expected utility theory when asked to decide whether to connect, or not to connect, to public Wi-Fi networks to execute the transactions. We noted that regardless of how much data plan/roaming the participants had, they did not select option that yield the highest expected utility. More participants made the same decision in the scenarios that took place overseas. In each scenario, the statistical binomial tests show that the proportion of participants making choices according to the expected utility theory deviates significantly ($p < 0.001$) from the presumed population value of 100% (Table 9 and 10). Therefore, there is sufficient evidence to reject the claim that people choose action that gives the highest expected utility, when deciding to connect, or not to connect, to public Wi-Fi, particularly for making financial transactions.

Table 9. Result from binomial test for case III and VII

Data plan level	Group[*]	Case III UK		Case VII Outside UK	
		N	Observed Prop.[**]	N	Observed Prop.[**]
100%	1	33	0.32	36	0.35
	2	69	0.68	66	0.65
75%	1	34	0.33	36	0.35
	2	68	0.67	66	0.65
50%	1	36	0.35	36	0.35
	2	66	0.65	66	0.65
25%	1	46	0.45	43	0.42
	2	56	0.55	59	0.58

Table 10. Result from binomial test for case IV and VIII

Data plan level	Group[*]	Case IV UK		Case VIII Outside UK	
		N	Observed Prop.[**]	N	Observed Prop.[**]
100%	1	24	0.24	20	0.20
	2	78	0.76	82	0.80
75%	1	24	0.24	21	0.21
	2	78	0.76	81	0.79
50%	1	24	0.24	19	0.19
	2	78	0.76	83	0.81
25%	1	30	0.29	25	0.25
	2	72	0.71	77	0.75

[*]Group 1 is a group of participants making choice according to the utility theory, Group 2 is a group of participants not making choice according to the theory.[**]All result significant at $p < 0.001$.

The results from binomial logistic regressions show a statistically significant correlation between the participants' decision making not in line with the expected utility theory and certain demographic factors, particularly gender, employment status, and perception toward security of public Wi-Fi in general.

a. Gender

Females are more likely to make choices not predicted by expected utility theory when asked to decide whether to connect, or not to connect, to public Wi-Fi networks. We noted statistically significant correlations in 11 instances across 6 scenarios. For examples, in Scenario II where participants were asked to connect to an open public Wi-Fi to make general non-financial transactions in an urgent situation in the UK, females were 7.02 times (β=1.95, OR=7.02, $p<0.05$) and 5.82 times (β=1.76, OR=5.82, $p<0.05$) more likely to not choosing the acts that would yield the highest expected value when they have 75% and 50% left on their mobile data allowance, respectively. Scenario VI presented a similar situation but, in this case, the scenario took place abroad. We noted that females also were 7.59 times (β=2.03, OR=7.59, $p<0.05$) and 7.27 times (β=1.98, OR=7.27, $p<0.05$) more likely to make choices not predicted by expected utility theory when they have 100% and 75%, respectively, left on their data roaming allowance.

Females are also more likely than male to decide to connect to public Wi-Fi, rating the likelihood that public Wi-Fi networks might be compromised higher (Table 11). When the scenarios located participants in the UK, despite having 100% and 75% left on data allowance plan, female were 3.67 times (β=1.30, OR=3.67, $p<0.01$) and 4.33 times (β=1.47, OR=4.33, $p<0.01$), respectively, more likely to decide to connect to public Wi-Fi to make non-urgent non-financial transactions. Similarly, for non-urgent financial transactions, female were 8.40 times (β=2.13, OR=8.40, $p<0.01$) and 5.84 times (β=1.77, OR=5.84, $p<0.01$) more likely to make the same decision when having 100% and 75% left on data plan, respectively. In case of urgent financial transactions, female were also 4.60 times (β=1.53, OR=4.60, $p<0.05$) more likely to connect to public Wi-Fi when they have 75% left on data plan allowance. However, for scenarios that placed participants outside the UK, this was only the case for urgent non-financial transactions. Female were 2.72 times (β=0.99, OR=2.72, $p<0.05$) more likely to use public Wi-Fi even when they have 100% of their data plan left (see Table 12).

Table 11. Perceived likelihood that public Wi-Fi can be compromised by gender (on a scale of 1-100%)

Location	Case	% that public Wi-Fi can be compromised		Mean differences
		Female	Male	
UK	I	48.80	37.64	11.16[*]
	II	50.35	40.21	10.14
	III	59.45	51.67	7.78
	IV	59.47	50.62	8.85
Outside UK	V	57.73	42.31	15.42[**]
	VI	55.95	44.62	11.33[*]
	VII	67.57	58.86	8.71
	VIII	67.35	56.79	10.56[*]

Table 12. Result from binomial logistic regression for the decision to connect to public Wi-Fi by Gender

Location	Case	Logistic probability of connecting to public Wi-Fi (Reference group = Female)			
		100%	75%	50%	25%
UK	I	3.66[**]	4.33[**]	5.27[**]	2.24
	II	1.53	2.60	1.53	1.41
	III	8.40[**]	5.84[**]	4.79[*]	2.32
	IV	3.75	4.60[*]	4.60[*]	2.36
Outside UK	V	1.40	1.77	1.31	1.06
	VI	2.72[*]	2.24	2.93[*]	2.69[*]
	VII	3.33	3.01	3.01	1.50
	VIII	1.44	1.18	2.14	1.32

[***], [**], [*] Significant at $p < 0.001$, $p < 0.01$, and $p < 0.05$, respectively.

b. Employment status

Students are more likely to make choices inconsistent with expected utility theory compared to unemployed individuals (the reference group). We observed a statistically significant correlations in 6 instances across 2 scenarios. For example, in case IV where participants were asked to connect to a public Wi-Fi network to make urgent financial transactions in the UK, students were 149.76 times (β=5.01, OR=149.76, $p<0.05$) and 462.72 times (β=6.14, OR=462.72, $p<0.05$) more likely to make choices inconsistent with expected utility theory when they have 100% and 75% left of their mobile data allowance, respectively.

In case V, on the other hand, where participants were asked to make a non-urgent non-financial transaction outside the UK, students were 55.05 times (β=4.01, OR=55.05, $p<0.05$) more likely to make choices inconsistent with expected utility theory when they have 50% left on their roaming data allowance. We noted that in Scenario III, where participants were asked to make financial transactions in a non-urgent situation in the UK, participants with a "part-time" employment status were 0.3 times (β=-3.38, OR=0.3, $p<0.05$) less likely to make choices inconsistent with expected utility theory than an unemployed individual.

c. General perception of public Wi-Fi security

We noted a statistically significant correlation between participants' perception of public Wi-Fi security and their choice of actions, inconsistent with expected utility theory, in 14 instances across 5 scenarios. For example, in case VIII, which we asked participants to decide to connect to a public Wi-Fi to make urgent financial transactions overseas, we found that for every 1% increase in the participants´ perception of riskiness, an individual is 0.92 times (β=-0.08, OR=0.92, $p<0.001$) and 0.93 times (β=-0.08, OR=0.93, $p<0.001$) less likely to make choices inconsistent with expected utility theory when they have 100% and 75% left on mobile data roaming, respectively.

In the next section, Section 5, we will discuss how we can apply the knowledge obtained from this study.

5. DISCUSSION

The following sections discuss the insight and possible future works from our study as well as the limitations. Each is discussed in turn.

5.1 Security and privacy implications

Our study confirmed that people still use unsecure public Wi-Fi, and that they take security risks in doing so – we found several examples of sensitive information being transmitted insecurely. These findings add further evidence to the result from previous studies which endorsed the extent of public Wi-Fi usage ([5], [12], [20], [23], [12], [29], [34], [35]) and the security and privacy implication from using such networks ([3], [7], [11], [12], [15], [33], [37], [39]).

We show that users can be vulnerable to privacy attacks when using public Wi-Fi. For users who may already be aware of the risks of using public Wi-Fi, the real-life privacy leak demonstrated in our study could help to further increase the level of their understanding. However, many of our participants assumed that public Wi-Fi within the UK is secure – perhaps because they assume that UK providers follow regulations or codes of practice and that users have trust in the environment they are familiar with [27]. We need to raise awareness that rogue Wi-Fi exists, that attackers impersonate trustworthy providers, and that even with reputable providers, there are security and privacy risks unless users deploy additional mechanisms, such as a Virtual Private Network (VPN). The risks they encounter while using public Wi-Fi is not visible, and most people do not realise that seemingly non-risky activities like browsing or search can reveal sensitive data. Installing privacy reminder software - such as the Wi-Fi Privacy Ticker, which displays information about sensitive terms that are sent from the user's devices, and prevents the unencrypted transmission of these terms – could help to raise awareness 'just in time' [13].

Understanding that people do connect devices to the network should be of concern to businesses who are adopting or thinking about deploying a BYOD ('Bring Your Own Device') policy. Under such a policy, users use the same devices for both business and personal purposes, potentially making corporate data vulnerable if users connect to insecure public Wi-Fi. Organisations should consider enforcing the use of VPNs when employees connect to corporate networks and ensuring that users are aware of the risks to corporate data when using their devices on public Wi-Fi networks.

To protect user security and privacy and to mitigate the risk of software developers failing to comply with data protection laws, the procedure to test software should be more stringent. It should include a comprehensive set of test cases to ensure that data will be transmitted securely not only on the wired network but also on public Wi-Fi network and mobile data. Previous studies have shown that users – faced with many competing demands on their time and cognitive resources - try to minimise to effort they expend on security ([19], [24]). The usability of security mechanisms is another challenge faced by users as many of those mechanisms create an overhead for users or are too difficult to use ([2], [30]). Therefore, the responsibility to protect the security and privacy of data should be placed more on the software providers. A recent good example is *WhatsApp* rolling out an automatic and inherent end-to-end encryption, so users do not have to make the decision of encrypting their conversations [40]. The same should be applied to other applications, particularly *Bumble*, the online dating app, we found to have leaked sensitive user information in our study.

The UK government may consider integrating the security and privacy risks from using public Wi-Fi to their existing cyber security awareness campaigns such as *Cyber Aware*[2] where, the advice about public Wi-Fi is very limited. The simple message could be – "*use your data plan for sensitive transactions- that's what it's there for*". The advice should also cover the scenarios when people go abroad - we found that participants are more likely to use public Wi-Fi to save money instead of paying for expensive data roaming. Perhaps, working with authorities responsible for transport hubs – could display ads to remind people of the risks of using free public Wi-Fi whilst on vacation. Demonstrations of how easy it is to set up a rogue Wi-Fi network and monitor people's traffic, as demonstrated in our study, would make the risks more visible (a similar approach was used by some broadband providers to convince home users to secure their routers). There are other tools that could be helpful - detecting an evil twin Wi-Fi access points can be performed using tools such as EvilAP Defender [45].

Public policy makers could use the evidence found in this study to establish rules and regulations to promote security and privacy on public Wi-Fi networks. First, as this study has demonstrated that data privacy could be compromised, the policy makers in the UK may consider analysing the pros and cons of allowing insecure

[2] www.cyberaware.gov.uk

public Wi-Fi to be set up as demonstrated in the German criminal court ordering all wireless owners to secure their networks by requiring passwords or registration for accessing in 2010. As of September 2016 [43], the European Court of Justice is still in favour of such decision and rule that open Wi-Fi hotspots need password to promote security.

5.2 Rationale for using public Wi-Fi

Our study provides empirical evidence that a significant proportion of participants' decisions about whether or not to connect to insecure public Wi-Fi network, are inconsistent with expected utility theory. This is an original piece of research exploring an aspect of decision-making not previously explored in studies investigating the decision-making process for using public Wi-Fi ([16], [17], [18], [22], [28], [38], [47]) or in more general studies of expected utility theory [46]. Our results are in line with behavioural economics literature which argues that expected utility theory is inconsistent with the styles of decision-making that people actually adopt in many real-life choice situations [25]. It supports criticism of expected utility theory, especially its assumptions that people are well behaved, and make rational, utility maximising choices [4] [42]. Behavioural economists argue that expected utility theory is associated with faulty predictions about people's decisions in many real-life choice situations and rational choice theory, whilst possibly the most influential economic theory of decision-making, fails to describe the world in which we actually live [25] [41].

Moreover, our novel contribution is that we were able to identify demographic and contextual factors that significantly influence participants to undervalue the security risks to preserve a resource that – rationally speaking – they have plenty of. In our survey, females were most likely to make risky choices even when they have 100% and 75% left on their mobile data plans and despite them perceiving a higher probability that public Wi-Fi networks can be compromised. This result contradicts with general perception and numbers of literatures observing greater risk-taking tendency in male ([9] [10] [21]). Possible explanations might be that women have lower levels of digital literacy and/or are less obsessive in their adoption of digital "hygiene" guidelines. A 'resource preservation heuristic', which mostly likely drives many of their daily decisions, has created a habit of trying to save their data plan whenever possible. Another driver is the plausibility that, in people's minds, quantifying lost from using mobile data allowance in monetary term is easier than quantifying potential lost from security/privacy breach caused by using free public Wi-Fi.

5.3 Future studies

The discovery of cookies leaking sensitive information whilst HTTPS is being used, whilst not completely new discovery, adds further evidence that HTTPS is not as secure as it is portrayed. In the case of *Bumble*, where the leak was observed in this study, date of birth and other sensitive information were pulled directly from the user's Facebook profile [8]. Therefore, the entire connection between the two applications should, in theory, be encrypted. Investigation into the root causes and remediation plan of these vulnerabilities presents an opportunity for future study. A similar study to explore any leaked information in different settings such as in developing countries where mobile usage is growing substantially whilst general cyber security is trying to catch up presents another research opportunity.

For the economics and security research community, the findings that participants in our study do not make choices as predicted by utility theory when deciding to connect, or not connect, to public Wi-Fi suggest that researchers need to consider the values that drive the behaviours of different demographic groups. Another area worth exploring is the sources of behaviour bias, which explains the divergence between the willingness to pay (WTP) and the willingness to accept (WTA) when people decide to use public Wi-Fi. Finally, investigating the resource preservation heuristic attitude and its effect on the risk taking behaviour in a wider computer security context is promising.

5.4 Limitations

Like other studies, our research has inherent limitations that readers should note when making any inference. First, for the public Wi-Fi monitoring experiment, the findings are based on data collected in central London which may not fully represent the behaviours of people outside London and outside the UK. Moreover, there may be more privacy leak from data transmitting through our experimental Wi-Fi but the keywords used to filter data during the analysis may not cater for it. The sample size for our interviews is relatively small, 14 in total. A larger sample size may be needed to represent the overall UK population.

For survey questionnaires, despite our efforts to promote good quality responses such as using engaging scenarios, enforcing data checks, randomising the order of the questions, and using fatigue test, there is an inherent risk that participants might not fully pay attention to the questions. And we are asking for hypothetical behaviour, rather than observing the behaviour itself. Also, for simplicity, we used a set of assumptions that may not always reflect real life. For example, we assumed that if user decides to connect to the Internet via public Wi-Fi, the connection will always work. This is not always the case in real life where experience has shown us that public Wi-Fi networks do not always work. Moreover, and perhaps most importantly, the nature of the questionnaires means that users may respond with what they think they would do, but they may behave differently in a real life scenario. For the econometric analysis, unravelling correlation and causation is problematic and some of the results may reflect influences from underlying variables. Fuller exploration of larger data-sets would give us more information about the ultimate causal factors.

Finally, the design of our study is restricted by the limitations faced by the expected utility theory approach and its assumptions implicit around risks which assume people have stable risk preference and do not have behavioural bias. Evidence from behavioural economics have consistently undermine such assumptions. The most prominent argument is the endowment effect whereby people perceive a loss of utility from giving up a valued good greater than the gain in utility from acquiring the same good, hence, creating a divergence between the willingness to pay and the willingness to accept [4].

In this section, we discuss the application of knowledge obtained from our study and the limitations in our study. The next section, Section 6, presents the conclusion.

6. CONCLUSION

We investigated the extent of public Wi-Fi usage and security and privacy implications from connecting to such networks using real life user generated data gathered from various locations in London, UK. We also examined reasons for using unsecure public Wi-Fi and bearing the risk of data being compromised, both from a quantitative approach based around expected utility theory, and a qualitative approach using user interviews.

We found that participants did connect to public Wi-Fi to perform various activities and that some applications and websites leaked

cookies that contained personal information. Further studies to understand the root cause and remediation actions for such failure presents a research opportunity. Examining rationale for using public Wi-Fi and bearing the risk of data being compromised shows that our participants, female in particular, indicated that they would use public Wi-Fi despite expressing concern over the security of the networks. Our findings that significant proportion of our participants make choices not predicted by utility theory supports a criticism made by behavioural economists that the expected utility theory fails to present a decision-making process of a 'real' human. Future studies to develop a more in-depth understanding of such behaviour in the context of public Wi-Fi security and information security, in general, are promising.

7. ACKNOWLEDGMENTS

Our thanks go to the Department of Security and Crime Science, the Department of Computer Science, the Bartlett School of Construction and Project Management at University College London, everyone participating in the study, and anonymous review comments. The authors were supported in part by UK EPSRC grants, no. EP/N033396/1.

8. REFERENCES

[1] Adamowicz, W. L. (1993). Experiments on the Difference between Willingness to Pay and Willingness to Accept Wiktor L. Adamowicz, Vinay Bhardwaj, and Bruce Macnab. Land Economics, 69(4), 416-427.

[2] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

[3] Aime, M. D., Calandriello, G., & Lioy, A. (2007). Dependability in wireless networks: Can we rely on WiFi?. IEEE Security & Privacy, 5(1), 23-29.

[4] Baddeley, M. (2012). Behavioural economics and finance. London: Routledge.

[5] Balachandran, A., Voelker, G. M., Bahl, P., & Rangan, P. V. (2002, June). Characterizing user behavior and network performance in a public wireless LAN. In ACM SIGMETRICS Performance Evaluation Review (Vol. 30, No. 1, pp. 195-205).

[6] Briggs, Rachael (2015), "Normative Theories of Rational Choice: Expected Utility", The Stanford Encyclopedia of Philosophy (Winter 2015 Edition), Edward N. Zalta (ed.).

[7] Brody, R. G., Gonzales, K., & Oldham, D. (2013). Wi-fi hotspots: secure or ripe for fraud. Journal of Forensic Investigative Accounting, 5(2), 27-47.

[8] Bumble, www.bumble.com/en-us/faq

[9] Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. Psychological bulletin, 125(3), 367.

[10] Charness, G., & Gneezy, U. (2012). Strong evidence for gender differences in risk taking. Journal of Economic Behavior & Organization, 83(1), 50-58.

[11] Chen, S., Wang, R., Wang, X., & Zhang, K. (2010, May). Side-channel leaks in web applications: A reality today, a challenge tomorrow. In 2010 IEEE Symposium on Security and Privacy (pp. 191-206).

[12] Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013, April). Characterizing privacy leakage of public WiFi networks for users on travel. In INFOCOM, 2013 Proceedings IEEE (pp. 2769-2777). IEEE.

[13] Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010, September). The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In Proceedings of the 12th ACM international conference on Ubiquitous computing (pp. 321-330). ACM.

[14] Evening Standard (2015), www.standard.co.uk/news/crime/cybercriminals-hack-into-free-wifi-hotspots-to-get-bank-details-a3151736.html

[15] F-Secure (2014), THE F-SECURE WI-FI EXPERIMENT, www.fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f-secure.pdf

[16] Ferreira, A., Huynen, J. L., Koenig, V., Lenzini, G., & Rivas, S. (2015, August). Do graphical cues effectively inform users? In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 323-334). Springer International Publishing.

[17] Ferreira, A., Huynen, J. L., Koenig, V., & Lenzini, G. (2014, June). Socio-technical security analysis of wireless hotspots. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 306-317). Springer International Publishing.

[18] Ferreira, A., Huynen, J. L., Koenig, V., Lenzini, G., & Rivas, S. (2013, September). Socio-technical study on the effect of trust and context when choosing wifi names. In International Workshop on Security and Trust Management (pp. 131-143). Springer Berlin Heidelberg.

[19] Florêncio, D., Herley, C., & Coskun, B. (2007). Do strong web passwords accomplish anything? HotSec, 7, 6.

[20] Hampton, K. N., & Gupta, N. (2008). Community and social interaction in the wireless city: wi-fi use in public and semi-public spaces. New Media & Society, 10(6), 831-850.

[21] Harris, C. R., Jenkins, M., & Glaser, D. (2006). Gender differences in risk assessment: why do women take fewer risks than men?. Judgment and Decision Making, 1(1), 48.

[22] Jeske, D., Coventry, L., & Briggs, P. (2,014, July). Decision justifications for wireless network selection. In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 1-7). IEEE.

[23] Hare, J., Hartung, L., & Banerjee, S. (2012, June). Beyond deployments and testbeds: experiences with public usage on vehicular WiFi hotspots. In Proceedings of the 10th international conference on Mobile systems, applications, and services (pp. 393-406). ACM.

[24] Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on new security paradigms workshop (pp. 133-144). ACM.

[25] Kahneman, D. & Tversky A. (1975), Judgment Under Uncertainty: Heuristics and Biases, New York: Cambridge University Press.

[26] Kern, B. D. (2004). Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. Santa Clara Computer & High Tech. LJ, 21, 101.

[27] Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. IEEE Security and Privacy Magazine, 10(2), 24-32.

[28] Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009, April). When i am on wi-fi, i am fearless: privacy concerns & practices in everyday wi-fi use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1993-2002). ACM.

[29] Lambert, A., McQuire, S., & Papastergiardis, N. (2014). Public Wi-Fi. Australian Journal of Telecommunications and the Digital Economy, 2(3).

[30] Mannan, M., & van Oorschot, P. C. (2008, July). Security and usability: the gap in real-world online banking. In Proceedings of the 2007 Workshop on New Security Paradigms (pp. 1-14). ACM.

[31] Market Watch (2015), www.marketwatch.com/story/how-dating-apps-are-getting-better-for-women-2015-08-12

[32] Neilson, W. S. (1993). An expected utility-user's guide to expected utility experiments. Eastern Economic Journal, 19(3), 257-274.

[33] Noor, M. M., & Hassan, W. H. (2013). Current threats to wireless networks. In The Third International Conference on Digital Information Processing and Communications (pp. 704-713). The Society of Digital Information and Wireless Communication.

[34] Powell, A., & Shade, L. R. (2006). Going Wi-Fi in Canada: municipal and community initiatives. Government Information Quarterly, 23(3-4), 381-403.

[35] Sathiaseelan, A., Mortier, R., Goulden, M., Greiffenhagen, C., Radenkovic, M., Crowcroft, J., & McAuley, D. (2014, December). A feasibility study of an in-the-wild experimental public access wifi network. In Proceedings of the Fifth ACM Symposium on Computing for Development (pp. 33-42). ACM.

[36] Schoemaker, P. J. (1982). The expected utility model: Its variants, purposes, evidence and limitations. Journal of economic literature, 529-563.

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

[38] Swanson, C., Urner, R., & Lank, E. (2010, June). Naïve security in a Wi-Fi world. In IFIP International Conference on Trust Management (pp. 32-47). Springer Berlin Heidelberg.

[39] Szongott, C., Brenner, M., & Smith, M. (2015, January). METDS-A self-contained, context-based detection system for evil twin access points. In International Conference on Financial Cryptography and Data Security (pp. 370-386). Springer Berlin Heidelberg.

[40] Tech Crunch (2016), WhatsApp completes end-to-end encryption rollout www.techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout

[41] Thaler, R. H. (1997). Irving Fisher: modern behavioral economist. The American economic review, 87(2), 439-441.

[42] Thaler, R. H. (2015). Misbehaving: The making of behavioral economics.

[43] The Register (2016), EU ends anonymity and rules open Wi-Fi hotspots need passwords, www.theregister.co.uk/2016/09/15/eu_ends_anonymity_and_rules_open_wifi_hotspots_need_a_password

[44] Transport of London (2016), Station Wi-Fi www.tfl.gov.uk/campaign/station-wifi

[45] Trip Wire (2015), How to Detect and Attack Evil Twin WiFi Access Points, www.tripwire.com/state-of-security/security-data-protection/detect-attack-evil-twin-wifi-access-points/

[46] Von Neumann, J., O. Morgenstern (1944), Theory of games and economic behavior, Princeton University Press, Princeton, NJ.

[47] Yevseyeva, I., Morisset, C., Groß, T., & van Moorsel, A. (2014, September). A Decision Making Model of Influencing Behavior in Information Security. In European Workshop on Performance Engineering (pp. 194-208). Springer International Publishing.

Appendix A: An example of case description and questions from scenario I.

You are waiting for a friend at a train station in the UK. When you arrive there, you see that the train is running 1 hour late. You want to check messages on messaging apps (e.g. WhatsApp) or emails on your mobile phone but you do NOT urgently need to contact anyone in particular. You last checked your messages about two hours ago. However, you do NOT have a data plan on your mobile phone.

Q: What is the maximum amount (per hour) would you be willing to pay to connect to the Internet in this scenario?

Suppose you decided to connect to free public Wi-Fi as described above and have connected successfully. At that point, before you actually use the Internet, the Wi-Fi router has reached its capacity and cannot accept any more user. However, successfully connected users, like yourself, can carry on with the connection without any problem. The Wi-Fi provider offers anyone who is willing to give up the connection a compensation in cash.

Q: What is the minimum amount (per hour) would you be willing to accept in exchange for giving up your Internet access?

Suppose you also have a 4G data plan on your mobile phone. You already have paid £10 for 1GB which has no expiration date. The 4G connection works properly. Using the Internet in this case will use about 100MB of your data plan (i.e. 10% of 1GB allowance).

Q: Would you connect to the Internet in this case, and via which means (i.e. data plan or free public Wi-Fi) when you have 100%, 75%, 50%, and 25% left on your data plan?

Q: From your perspective, what is the likelihood (1-100%) that security could be compromised when using mobile data plan to connect to the Internet in this case?

Q: From your perspective, what is the likelihood (1-100%) that security could be compromised when using free open public Wi-Fi to connect to the Internet in this case?

Suppose you can connect to the Internet securely by using an end-to-end encryption service like Virtual Private Network (VPN). However, you have to pay for such a service.

Q: What is the maximum amount (per hour) would you be willing to pay for such a service?

Q: What is the minimum amount (per hour) would you be willing to accept in exchange for giving up secure Internet connection?