information

MDPI

Article

Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumptions of Mobile Device Users

Bram Bonné *, Gustavo Rovelo * , Peter Quax * and Wim Lamotte *

Hasselt University—tUL—imec, Expertise Centre for Digital Media (EDM), Wetenschapspark 2, 3590 Diepenbeek, Belgium

* Correspondence: bram@brambonne.com (B.B.); gustavo.roveloruiz@uhasselt.be (G.R.); peter.quax@uhasselt.be (P.Q.); wim.lamotte@uhasselt.be (W.L.)

Received: 8 May 2017; Accepted: 28 June 2017; Published: 1 July 2017

Abstract: Smartphones and other mobile devices have proliferated in the past five years. The expectation of mobile device users to always be online has led to Wi-Fi networks being offered by a variety of providers. Using these networks introduces multiple security risks. In this work, we assess to what extent the privacy stance of mobile device users corresponds with their actual behavior by conducting a study with 108 participants. Our methodology consists of monitoring Wi-Fi networks that the participants' devices connect to and the connections made by apps on these devices, for a period of 30 days. Afterwards, participants are surveyed about their awareness and privacy sensitiveness. We show that while a higher expertise in computer networks corresponds to more awareness about the connections made by apps, neither this expertise nor the actual privacy stance of the participant translates to better security habits. Moreover, participants in general were unaware about a significant part of connections made by apps on their devices, a matter that is worsened by the fact that one third of Wi-Fi networks that participants connect to do not have any security enabled. Based on our results, we provide recommendations to network providers, developers and users on how to improve Wi-Fi security for mobile devices.

Keywords: privacy; security; wireless networks; usability; 802.11; user study; security practices; security awareness; mobile

1. Introduction

Smartphone and other mobile device usage has increased greatly in the past years: data from Eurostat shows that over the past five years, the number of individuals in the EU aged 16 to 74 that are using a mobile phone to access the internet has increased from 19% in 2011 to 56% in 2016 [1]. Similarly, in emerging economies such as Malaysia, Chile, Brazil and Turkey, smartphone ownership rates have increased by more than 25% in two years (with an increase of 42% in Turkey) [2]. Together with mobile devices, Wi-Fi networks have become more prevalent, often being offered by either commercial or public entities as a service to their customers. Connecting to the internet using one of these Wi-Fi networks entails some form of trust: the connections themselves—and, in case these connections happen unencrypted, their data—can be monitored by the provider of the network. Moreover, the provided networks often lack any form of security, with previous studies showing that 45% of 1404 encountered smartphones were set up to automatically make a connection to at least one insecure network [3]. This allows not only the network provider, but also others within range of the network to eavesdrop on communications. Having access to this information can allow for third parties to generate a highly accurate profile of mobile device users, which entails inherent privacy risks [4].

The problem of security is worsened by the fact that not all apps are using secure methods of connecting to the internet. Indeed, if apps fail to implement proper end-to-end encryption, eavesdroppers are able to see the data sent by these apps on an insecure Wi-Fi network. In 2012, Georgiev et al. showed that even when apps are using secure (SSL) connections, they often fail to validate certificates correctly, opening the door to active man-in-the-middle attacks [5]. This means that providers of Wi-Fi networks would be able to intercept data, even if encryption is used. The researchers uncovered faulty certificate checking in libraries for cloud computing (e.g., EC2), web services (e.g., Apache Axis), merchant sof tware development kits (e.g., PayPal), and ad libraries (e.g., AdMob).

Data from Eurostat further shows that 48% of internet users had been limited or kept from performing an internet activity (e.g., buying goods or providing personal information to online communities) due to security concerns during the 12 months prior to a 2015 survey. However, only 13% of these users had limited their internet use because of security concerns when accessing the internet on a mobile device via a wireless connection from places other than home [1].

In the past, researchers have studied the amount of privacy and security awareness of Wi-Fi users, with one of the more notable studies being performed by Klasnja et al. in 2009 [6], where laptop users were surveyed about their network usage and corresponding privacy concerns. These studies show that user expectations of privacy often do not correspond to the reality, and that a person's stance towards privacy often does not correspond to their actual behavior [7].

Our study expands on this earlier work but updates the methodology to deal with the changing technology landscape. On one hand, it aims to assess whether mobile device users are aware of the network connections that are being made over Wi-Fi by installed applications (possibly in the background). On the other hand, it tries to find out how comfortable these users are with the fact that this application data is sent over the Wi-Fi network they are connected to, allowing it to be monitored by either the network operator, an eavesdropper (in the case of unsecured networks and connections), or both. We only consider the use of Wi-Fi networks to access the internet by mobile device users, and not the Wi-Fi connections that are used by network providers to access their backbones.

With this, we aim to assess whether the changed security and technology landscape has led to a change in security perceptions and practices between 2009 and 2017. We aim to get an idea of whether the principles of visibility ("The interface should allow the user to easily review any active actors and authority relationships that would affect security-relevant decisions") and trusted path ("The interface must provide an unspoofable and faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf"), as defined by Yee [8], are satisfied for current mobile device users.

2. Related Work

This study is mainly influenced by work from Klasnja et al. [6], in which participants' network usage is monitored. Part of the study consisted of showing participants a list of web sites to which specific bits of personal information were sent unencrypted, asking the participants about their awareness on the transmitted information, and how they felt about it. Klasnja et al. observed that four out of the eleven participants were aware that other people could possibly access their information being transmitted over Wi-Fi, but that this understanding did not raise concerns. Our study works in a similar way to this work but updates its methodology to deal with the changing technology landscape where mobile devices are rapidly surpassing notebooks in usage [9]. The revised methodology uses smartphones and tablets as the main devices, and envisions to gather more quantitative rather than qualitative data with a participant pool of $N = 108$. Our approach also considers only the connection metadata (such as the originating app and the connection endpoint), rather than the actual transmitted data.

After the study by Klasnja et al., Consolvo et al. introduced the "Wi-Fi Privacy Ticker" [10]. This tool informs users about sensitive data being sent out over their wireless interface, while indicating whether the connection is secure. The results of their study show that the ticker helped participants

to increase their awareness, and that it helped participants form more accurate mental models of the circumstances in which data gets transmitted, eventually contributing to changes in user behavior while on Wi-Fi. In our work, we try to (i) assess the level of awareness (without actively raising awareness) and (ii) determine if this awareness has a positive impact on security habits.

A study from 2010 by Swanson et al. [11] reported on the perception of privacy and security when using wireless networks for a group of 11 randomly selected persons. They show that users make security choices based on (often mistaken) analogies to the physical world, similar to what happens in naïve, or "folk" physics, and that this leads to users who are confident in their knowledge about security while making unsafe decisions. They call this phenomenon "naïve risk mitigation", providing examples of participants trusting a connection because they trust the company they are interacting with, or participants believing a malicious actor would not have the time to sort through all the data that could be gathered. Their survey also included an educative component, as it explained the associated risks of such actions to the participants. This study shows the need for concrete examples of network scenarios when surveying device users about security of their data. We apply this in our own work by having the survey questions represent concrete scenarios of applications sending data over wireless networks, with both the applications and the networks corresponding to those used by the participants.

Even when people think of themselves as privacy conscious, their actual behavior often does not match their intentions. Norberg et al. describe "The Privacy Paradox" as the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behavior [7]. They find that individuals will actually disclose a significantly larger amount of personal information than their stated intentions indicate.

Like privacy stance, there does not seem to be a direct relationship between a person's technical background and the actions they take to control their privacy or increase their online security. In a 2015 study, Kang et al. use diagramming to determine users' mental models about the internet, and conclude that individuals' technical backgrounds do not influence their privacy or security behavior [12]. Our study tries to assess whether these findings also apply to users of Wi-Fi networks, by looking for correlations between technical level and privacy intentions of the participants, and the security of networks to which they connect.

In 2012, Chin et al. analyzed the confidence smartphone users had in smartphone security and privacy [13]. The study finds that participants are less likely to perform certain privacy sensitive activities on their smartphones than on their laptops, finding, e.g., a difference of 7% vs. 60% of participants not willing to entering their social security number. With the study being performed in 2012, participants cited reasons such as "new phone technology" for not trusting their mobile devices with privacy sensitive information. However, some participants also noted not trusting the Wi-Fi network, or mentioned "potential hackers hanging out in cafes". These results seem inconsistent with a Eurostat survey from 2015, where only 13% of participants had limited their internet use because of security concerns when using the internet with a mobile device via a wireless connection from places other than home (compared to 70% in total) [1]. This could indicate that the technology landscape has changed considerably since 2012, with smartphones becoming a more integral part of people's lives.

A more recent study from Clark et al. shows that users of internet services are often unaware about which of their data is transmitted to the cloud and stored there, using GMail's attachment storage as an example [14]. They show that task-oriented users rarely stop to think about the security implications of their actions. Their results suggest that the same might apply to wireless network users, quickly connecting to a free Wi-Fi hotspot in order to perform a task at hand (e.g., to get to a website containing information needed at that moment).

With these studies indicating a possible discrepancy between users' privacy attitudes and behaviors between five years ago and now, our goal is to assess to what extent the shift from personal computers and laptops to smartphones has impacted these privacy properties. Moreover, we want to find out whether the Privacy Paradox also applies to mobile device users in 2017. Our main

contribution can hence be summarized as the answer to the question: with a security landscape that changed significantly since 2009, did privacy perceptions and practices change with it?

3. Methodology

Our study consists of two phases: first, network connections made by apps on the participant's phones over Wi-Fi are logged for four weeks. Afterwards, the participants need to answer an exit survey containing personalized questions about their privacy preferences and the logged connections. For the remainder of this paper, we will talk about "connections" as the actual (transport layer level-) connections that are made by apps on participants' devices to a server on the internet. Associations between a mobile device and a Wi-Fi access point will be referred to as "networks".

3.1. Connection Monitoring

In the first phase of the experiment, participants are asked to install an Android application which does not contain any user interface except for a welcome screen that tells the user to exit the app and to leave it installed for the duration of the study. This application runs in the background, collecting information about which Wi-Fi networks the participant connects to, and which network connections were made by apps on these networks. More specifically, the data logged for Wi-Fi networks is:

- The network name (SSID)
- Whether the network provides any security in any form; either Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or WPA2

Note that both WEP and WPA have been proven to have major security weaknesses [15], and that their use has been discouraged in favor of using a more modern and secure protocol such as WPA2 for wireless security. For the sake of this study, we do not differentiate between different types of security. Instead, we will focus on networks without any security enabled, for which we are certain that eavesdroppers are able to capture traffic that is sent in the clear.

Furthermore, for every connection made by any of the apps installed on the phone, the following data is logged:

- The app name (visible to the user) and package name (unique for every app) for the app making the connection
- Whether this app is launchable by the user, as some (system) apps run in the background without being visible to the user
- The hostname (or the IP address, in case no hostname can be resolved) and port of the connection's endpoint
- A timestamp of when the connection is made
- The Wi-Fi network the device is connected to when the connection is made

Only the connection metadata is recorded; no actual communication (i.e., messages, e-mails or any other app content) is gathered by the monitoring app.

The data is gathered by periodically reading and parsing Android's `/proc/net/tcp` and `/proc/net/tcp6` files and matching the user IDs for each connection to a corresponding app on the participant's device, only while the device is connected to a Wi-Fi network. In contrast to how the usual sandboxing model of Android is implemented, apps can view the connections made by other apps by reading these files. Both reading these files and resolving the user IDs or the names of the apps do not require any permissions to be requested by the monitoring app. The only permission that needs to be granted by the user is to view the names and properties of Wi-Fi connections, a requirement of which the participants are informed beforehand.

Since the connection monitor is only periodically logging connections (once every 15 min), some of the connections might be missed. Even though this only applies to connections that have been opened, closed, and passed their `TIME_WAIT` timeout of 4 min all within the timeframe of 15 min,

we take our gathered data to be a lower bound on the actual number connections made. Since we only use apps, not individual connections, as part of the study, this should be representative for the actual connections made by the device. Moreover, logging happens using Android's `AlarmManager`, which is set up to log "inexactly", causing logs to happen together with other jobs (such as another app syncing data). This mitigates the fact that logging does not happen continuously by making sure it happens at the most "busy" moments.

Apart from logging the aforementioned data, the app also shows a mini-survey whenever the participant connects to a wireless network they never previously connected to. This survey asks the participant to provide a one-line description about the network, aiding the participant in remembering the specific network or situation during the exit survey. An example of such a scenario is when the participant is on holiday in an unknown city, and connects to the free Wi-Fi network in a bar. In this case, he or she can provide a short summary about the place providing the network (e.g., "small bar with friendly owner next to the train station"), or about the reason (e.g., "needed to look up the location of a restaurant nearby").

Participants are given instructions for installing and activating the app on their own personal devices, and for whitelisting the app from any "battery saver" or "memory cleaner" apps that might interfere with its operation. The app is distributed through the Google Play Store, with its availability being limited to only participants of the study. Data collection happens for a period of 30 days for every participant, with the researchers and recruiters following up with participants to make sure the app was functioning correctly. This includes making sure the app is consistently transmitting data, indicating it was not suspended or terminated by any "optimizer" app, and that the aforementioned whitelisting is done properly.

At the end of the connection monitoring phase, connections made to third-party advertising servers are excluded from the dataset. The reason for this is that the connection monitor is only able to view the connections made by other apps, without being able to see the type of data that is being transmitted. Because of this, some apps might have only sent non-service specific metadata (such as device identifiers used for advertising). To identify hosts that are used for serving ads instead of content, we use the hosts file that is part of the popular AdAway ad-blocker for Android (The AdAway hosts file is available at [16]). This file contains an exhaustive list of hosts that are used to serve advertisements to Android apps and to gather analytics data from users of Android apps. By applying this filter, 10.05% of a total of 5,780,105 connections are removed from the dataset, which excludes 295 distinct $(network, app)$ pairs (1.23% of a total of 24,030).

3.2. Exit Survey

The exit survey is provided to the participants at the end of the experiment, and consists of two parts: a survey containing personalized questions based on the gathered data, and a general (non-personalized) survey containing questions about the participant's privacy stance.

3.2.1. Personalized Questions

The first part is based on the data gathered during the first phase of the experiment. For every participant, personalized questions are generated based on a subset of both the connections and Wi-Fi networks. These questions (available in Appendix B) are designed to poll the participant about their privacy stance towards the data for a particular app on their phone being accessed by either the network operator or an eavesdropper (in the case of open networks). The process of selecting and generating these questions is outlined here.

For every participant, three networks for which connections occurred during the monitoring phase are selected programmatically. Our program is configured to give a preference to unsecured networks, as they allow for extra survey questions (see below). Moreover, the number of "hotspots provided by internet providers", where an internet provider rolls out a nationwide network based on Wi-Fi hotspots, is limited to at most one. As hotspots are the most prevalent unsecured networks

based on number of connections made (see Section 6), including them all while giving preference to unsecured networks would yield a set of responses that is heavily biased towards these internet service provider (ISP) hotspots. Apart from these two preferences, networks are selected completely at random.

For each of the selected networks, three apps that made a connection to a first-party server (i.e., a server not belonging to a third-party advertiser) while being connected to the network are selected, creating a total of nine $(network, app)$ pairs. Before this selection happens, a few apps are excluded from the list. These apps include web browsers, system apps, and other supporting apps (such as Google Play Services) because a participant might be unable to formulate a meaningful response to posed questions, skewing the results in the process.

Our program is again configured to select apps based on a few preferences. First, if possible, at least one connection involving a messaging app (such as Facebook Messenger, WhatsApp or Telegram) is included as part of the questions (The messaging apps are selected from the list of top free apps in the *Communication* category on Google Play [17]). This allows to compare answers for a specific app category afterwards. Second, as was the case with the network selection, a preference is given to insecure connections. For insecure $(network, app)$ pairs, one additional question is added to the survey, asking the participant to what extent they would mind an eavesdropper being able to see app data (cf. question *Q7* in Appendix B). Only when no more "insecure pairs" (apps making an insecure connection on an open network) are available, secured connections are selected. Apart from these preferences, apps are selected completely at random.

Note that the previously outlined selection only applies to the questions themselves. Results listed in later sections will always apply to the full dataset (excluding connections made to advertisement networks), unless otherwise noted.

For every network, the participant is shown a small one-line summary that they provided themselves as part of the mini-survey occurring during connection monitoring (see Section 3.1), together with the exact time at which the first connection to this network was made. We display the connection time for the first connection (instead of a later connection) because this is the time at which the participant filled in the mini-survey, and because this is a connection that was actively initiated by the participant; later connections may have been made automatically by the device, while the first connection was made with a specific purpose in mind.

Even though all of these questions are based on actual connections made by apps installed on the participants' devices, they are not informed about this. Instead, the connections are presented as hypothetical scenarios, asking only about the extent to which participants would agree with this data being visible to one of the aforementioned parties. This ensures that participants' responses are not influenced by the actual data. The last question for every connection asks about how high the participant would estimate the likelihood that the connection actually occurred. In addition to this, the very end of the survey contains the same question in a more direct form, informing the participant about the fact that this connection effectively happened.

The hostname and address of the endpoint the app connected to are only used for statistics. We chose not to include this information as part of the survey because a substantial fraction of these connections are made to a content delivery network or a cloud provider (e.g., Amazon Web Services) where the back end for the app is hosted: a cursory search shows that at least 14.92% of the logged connections belong to one of a few popular cloud providers like amazonaws.com or akamai.net.

We consider connections made to TCP port 80 to be unencrypted. In principle, an app could create a secure connection to TCP port 80 either by using HTTPS over this port (instead of the default HTTPS port 443), or it could implement its own secure protocol on top of unencrypted HTTP connections. Since network connection monitoring on non-rooted Android devices does not provide access to the actual data on the connection (only the connection's meta-information), and, because encrypted traffic over TCP port 80 is highly uncommon [18], this assumption is deemed to be valid for the purpose of this study.

3.2.2. General Privacy Questions

The second part of the exit survey assesses the participants' general privacy stance. For this purpose, the survey contains questions from a 2014 study conducted by Pew Research, which polls participants about their privacy and personal information [19]. More specifically, questions Q11 and Q12 from the Pew Research study are used to ask the participant about which privacy-enhancing technologies and habits they know of, and which ones they have used or carried out before. Some examples of such technologies and are "using a temporary username or email address", "encrypting phone calls, text messages or email" and "clearing cookies and browser history".

The privacy questionnaire is included in the exit survey instead of being part of the onboarding questionnaire in order to avoid influencing participants' privacy behavior during the study. Care is taken to prevent participants from knowing beforehand that the study is about privacy, instead framing the study as a more general "study about wireless networks". Moreover, asking the questions about the participants' privacy stance is deferred until the very end of the exit questionnaire in order to avoid influencing the answers to questions pertaining to app data.

4. Participants

Participants are recruited through an external recruitment organization, with the aim of having a participant pool that is as diverse as possible. The participant pool's diversity is controlled by technical knowledge, education level and demographics, assessed by the questions in Appendix A. Participants are offered an incentive of €15 for completing the experiment. As explained in the previous section, the study is labeled as a general "study about wireless networks" to prevent participants from knowing beforehand that the study is about privacy issues in wireless networks. All communication with the participants is framed accordingly.

After removing participants that did not complete the full study (either because they did not keep the monitoring app installed for 30 days or because they did not complete the exit survey), the participant pool contains 108 Belgian people aged from 18 to 65 (a full age distribution of participants is available in Table 1a). Thirty participants identified as female, and 77 identified as male. Most participants completed a master education or higher (a full distribution of the participants' education is available in Table 1b). When asking to rate their technical expertise, most participants (44%) say they have a "high" or "very high" knowledge about how computer networks work, with only 13% rating their knowledge "low" or "very low". This corresponds to responses for the question "Would you be able to explain what WEP, WPA and WPA2 are?", controlled by a question to effectively provide the explanation, where 66% of participants indicate they would be able to provide this explanation. We found a strong correlation between the declared technical expertise and the participants being able to change a Wi-Fi network's settings (Pearson's $r(106) = 0.49$, $p = 6.62 \times 10^{-8}$) and to participants being able to explain how Wi-Fi security works (Pearson's $r(106) = 0.59$, $p = 4.42 \times 10^{-11}$).

For sake of completeness, we also controlled the correlation between the declared expertise and a more strict validation of the explanations about Wi-Fi security. After adjusting the category of 15 participants that did not explain Wi-Fi security entirely correct (e.g., by describing the encryption standards as only authentication mechanisms), we can still observe the same trend in the correlation between the declared expertise and whether participants were able to explain Wi-Fi security or not (Pearson's $r(106) = 0.45$, $p = 1.114 \times 10^{-6}$).

In conclusion, the participant pool is skewed towards relatively young (18–35 years), male, highly educated people with a high expertise in computer networks. In Section 6, the impact of this bias on the results is discussed in more detail.

Table 1. Participant statistics.

(a) Age Distribution.	
Age Group	**# Participants**
18–25	31
26–35	43
36–45	18
46–55	7
56+	4
Undisclosed	5
(b) Education Level.	
Highest Completed Education	**# Participants**
Master degree or higher	56
Bachelor degree	33
High school degree	17
Did not finish high school	2

5. Results

During the 30-day connection monitoring study, users connected to an average of 8.02 Wi-Fi networks, with the vast majority of users (61%) connecting to anywhere between 4–8 networks (see Figure 1). This shows a larger than 100% increase compared to the study performed on notebooks instead of smartphones by Klasnja et al. in 2009, where the average user connected to four networks during a period of four weeks. In addition, 310 of the 866 networks that devices connected to (35.8%) did not have any security (in the form of WEP, WPA, WPA2 or WPA2-enterprise) enabled. All of the participants connected to at least one secured network, which shows an improvement in security compared to Klasnja's study in 2009, where four out of 11 participants only connected to unsecured networks. Even so, as mentioned in Section 3.1, a network having security enabled does not necessarily mean the network is secure. Indeed, WEP and WPA have been proven to have major security weaknesses. A Pearson correlation test did not show any statistically significant correlation between the expertise of the participants and the number of unsecured networks they connected to during the experiment. Furthermore, our results show there is no statistically significant correlation between participants' privacy stances (measured by the number of positive answers to the questions defined in [19]) and the number of unsecured networks they connected to during the experiment. A general overview of the collected data is available in Table 2.

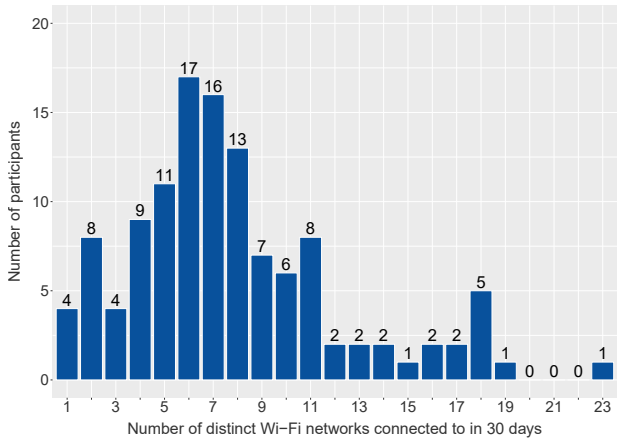

Figure 1. Number of Wi-Fi networks connected to by participants during the 30-day study. On average, participants connected to eight networks, with the vast majority of them (61%) connecting to anywhere between 4–8 networks.

Table 2. Statistics for the collected data.

Number of...	Amount
Participants	108
Wi-Fi networks	866
Open Wi-Fi networks	310 (35.8%)
Distinct apps	1667
Connections	5,330,660
Insecure connections	688,930 (12.9%)
Distinct *(network, app)* connection pairs	23,735

After accounting for the fact that the number of ISP hotspots was artificially limited in the questionnaire (by removing these 51 networks from the list of 311 networks participants were surveyed for), the two most prevalent types of networks that were part of the questionnaire were commercially offered Wi-Fi networks (belonging to e.g., a cafe or a supermarket) and own home routers, together accounting for just over 50% of all encountered networks (see Figure 2).

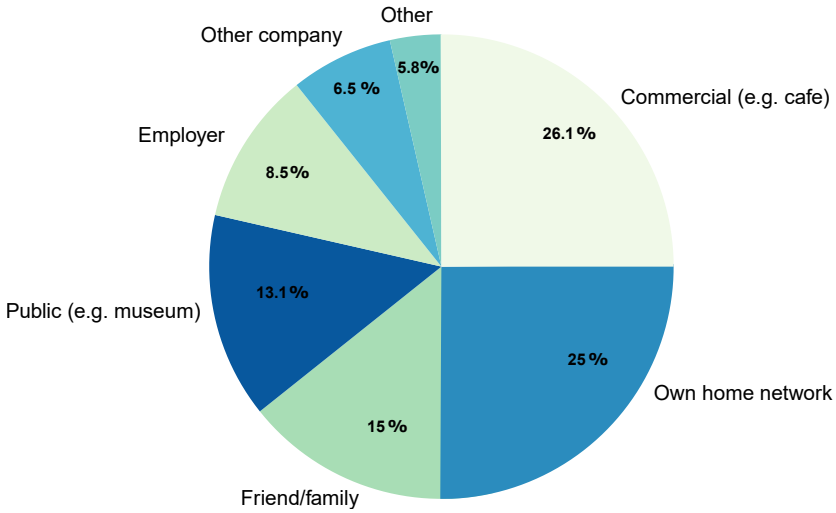

Figure 2. Distribution of the different types of networks in the survey. Excluded from this distribution are 51 networks having the "ISP hotspot" type, as these were purposefully limited to at most one (see Section 3.2 for more information). The two most prevalent types of networks that were part of the questionnaire were commercially offered networks and own home routers, together accounting for just over 50% of all encountered networks.

Participants indicated on multiple occasions that they were unsure about the identity of networks they connected to, indicating this either as part of the general survey feedback (*"My responses on [network X] are not reliable, as I don't know this network"*) or at the moment they are connecting to the network (by giving a one-line summary along the lines of *"No idea"*, *"Unknown network"* or *"Don't know this"*).

The participants' devices had an average of 65.44 apps making a connection to an external server during the experiment, with most devices (60%) having between 30 and 70 apps connecting over this period (see Figure 3).

Participants were often surprised about connections being made by apps, indicating that they were unaware about 345 of 928 (38%) connections that were surfaced as part of the exit survey. Excluding messaging apps (where participants indicated awareness for 72% of the connections being made), this number grows to 264 out of 629 apps (or 42%). This also showed in the general feedback given at the end of the study, where two participants talked about a mismatch in privacy expectations and actual behavior. One participant explicitly noted *"It surprises me that Skype transmitted data, as I did*

not configure the app yet", while another user's privacy expectations did not align with what the app was actually doing, as indicated by their feedback *"When surfing anonymously, the 'incognito' mode of Google Chrome that I use regularly was seemingly not taken into account"*. Another participant explicitly indicated that the survey caused them to take action, providing as feedback: *"Interesting survey. I'll certainly remove FileExpert from my device now."*. In this regard, we found a medium correlation between the declared expertise of participants and how aware they were about the connections being made (Pearson's $r(106) = 0.34$, $p = 2.09 \times 10^{-4}$). Figure 4 shows the distribution of the awareness count depending on the expertise of the participants.

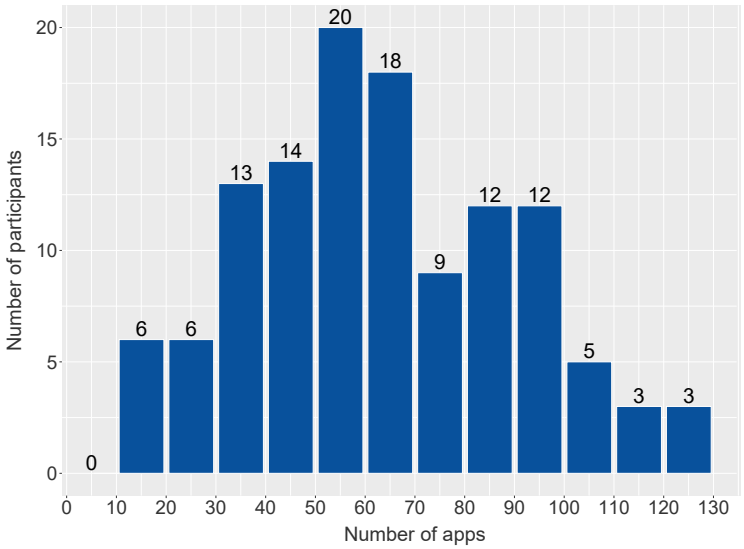

Figure 3. Number of apps on participants' phones making a connection to an external server during the 30-day study, grouped in bins of 10. The majority of devices (60%) have between 30 and 70 apps making a connection to the internet over this period.

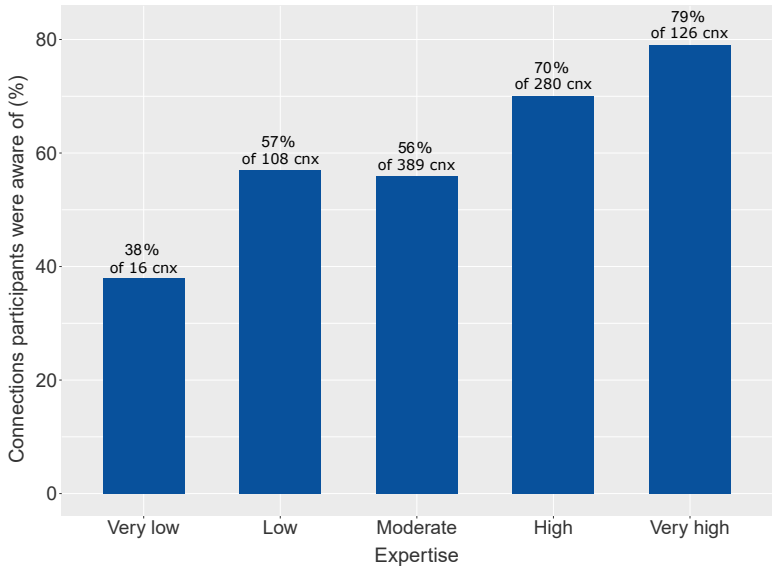

Figure 4. Number of times participants indicated to be aware of connections being made by the apps according to their expertise in computer networks. Participants with a higher expertise indicated to be more aware on average about the connections made by the apps installed on their devices.

Of the 321 insecure connection pairs ($(network, app)$ pairs containing both an insecure Wi-Fi network and an unencrypted connection made by the app), participants responded for 292 cases (91%)

that they would not want a person in the neighborhood of the Wi-Fi network being able to see the data sent over the connection, stating they either *disagree* or *strongly disagree* with the statement "A random person in the neighborhood of <network name> (e.g., someone standing on the street close to the building) is permitted to see all information (see previous question) of app <appname>". This could indicate that participants were not aware about the security risks inherent to connecting to open networks, or that they were unaware about the app making an insecure connection (remember that connections made to advertisement networks were not used for any survey questions, as explained in Section 3.1) on this network.

Even when asked about the extent to which the network owner would be permitted to see data transmitted by the apps that actually transmitted data over the network, 655 out of 928 connection pairs (71%) were deemed by participants to contain data that would be too sensitive for the network owner, indicated by answering that they "disagree" or "strongly disagree" to the statement "The owner of <network name> is permitted to see all information (see previous question) of app <appname>". This number even increases to 88% if we only consider the 191 hotspot networks provided by ISPs, which we hypothesize could be the case because participants may be considering these hotspots as belonging to an unknown person's home network. The data analysis showed a small correlation between the expertise of participants in computer networks and their concern about the network owner seeing the transmitted data (Person's $r(926) = 0.07$, $p = 0.04$).

We also analyzed the effect of the type of data (username, password and data such as instant messages, emails or weather information) on the privacy concern level of participants in our study. To measure participant's privacy concern, we use a 5-point Likert scale for the security concern rating, where 1 corresponds to "Not at all concerned", and 5 corresponds to "Extremely concerned". The Shapiro–Wilk and Barlett's tests show that the data violates the normality and homogeneity of variance requirements to perform an ANOVA test. Thus, in this case, we use the Friedman non-parametric test for the comparison among the groups (considering that one participant contributes to the sample with multiple records, we use a within subjects design). The Friedman test reveals a significant effect of the type of data on the privacy concern of the participants when using a mobile app ($\chi^2(3) = 240.5$, $p < 2.2 \times 10^{-16}$). A post hoc test using Mann–Whitney tests with Bonferroni correction shows significant differences between privacy concerns for the username and data, and username and password. Participants rated the privacy concern for the username the lowest ($avg = 1.48$, $SD = 1.06$), followed by the password ($avg = 2.21$, $SD = 1.61$), and gave the data the highest privacy concern rating ($avg = 2.30$, $SD = 1.43$).

Given the wide variety of applications that made a connection from the smartphones of the participants, we performed the same analysis considering only applications in the *Communication* category (i.e., messaging apps). As explained in Section 3.2, we selected at least one application of this type (if one was available) when generating the survey questions. The results of the analysis follow the same trend as those observed for the full dataset: the Friedman test reveals a significant effect of the type of data on the privacy concern of the participants ($\chi^2(3) = 241.12$, $p < 2.2 \times 10^{-16}$). A post hoc test using Mann–Whitney tests with Bonferroni correction again shows significant differences between privacy concerns for the username and data, and username and password, with similar differences (username: $avg = 1.53$, $SD = 1.03$, password: $avg = 2.38$, $SD = 1.61$, data: $avg = 2.63$, $SD = 1.50$).

6. Discussion

Our results show some interesting trends, both in terms of data gathered about participants' mobile device Wi-Fi usage, as in terms of their privacy and security awareness and concerns. This section provides some general remarks and further insights derived from the results.

First, this research was purposefully limited to connections on Wi-Fi networks because of the many inherent risks involved: these networks are often operated by small businesses, and security can be lacking. However, as mobile data is getting cheaper, more smartphone users are using their cellular network to connect to the internet. This is also indicated by the study's participants, with comments

such as *"I'm connecting to (public) wifi predominantly when I'm abroad, as I have a good data-subscription domestically and I trust my mobile provider more than I trust public networks."* and *"This research was about public wifi. I still use this, but not as much as I used to when I had a tablet that only had wifi. Now that I have a data subscription I use [Wi-Fi networks] a lot less. The security of mobile data connections seems more relevant to me now"*. Even so, our results show that mobile device users in 2017 are still relying on Wi-Fi for a significant amount of their internet access, with the majority connecting to 4–8 different Wi-Fi networks in 30 days. Adding to this is that a large part of Wi-Fi usage can be attributed to ISP hotspot networks, together accounting for over 94% of all connection pairs that were logged by the monitoring app (Because connections are only logged periodically, they provide only a representative subset of all connections made by the device. See Section 3.1 for more information on why this is still relevant.).

It is important to note that over one third (35.80%) of Wi-Fi networks participants connected to were insecure, allowing eavesdroppers to monitor metadata about network connections and—when the connections themselves are unencrypted – their actual data. Moreover, it facilitates malicious actors into mounting so-called "Evil Twin" attacks, where an existing (unsecured) network in the victim's preferred network list is spoofed by an attacker, causing the victim's device to automatically connect to the malicious network [20]. Combined with the fact that 12.92% of logged connections (excluding servers of advertisement agencies) were insecure, this presents a real security risk. When considering all networks (even those filtered out for the survey), the biggest offenders seem to be commercial entities (35.75% of open networks) and hotspots provided by the ISP of the home network (23.46% of open networks). This indicates that, even in 2017, Wi-Fi network security should still be considered an important topic in research and in the industry.

As is clear from Section 4, the participant pool is skewed towards highly educated people with a high expertise in computer networks (even though this expertise is self-reported, it was cross-checked with their ability to explain network security; see Section 4 for more information.). This leads to the expectation of participants being more aware about the apps operating on their devices than the general public, and to their expertise in computer networks having a positive impact on their security habits. Our analysis does indeed show that participants reporting a high expertise in computer networks are slightly more aware about connections being made, confirming expectations. Nonetheless, even participants reporting a "high" or "very high" expertise in computer networks were still unaware about 36.70% of connections made by apps on their device.

More surprising is that this expertise in computer networks does not seem to translate to better security practices: having this expertise did not prevent participants from connecting to as many unsecured Wi-Fi networks as less technically experienced participants. This confirms prior results from Friedman et al. [21], who found that high-technology participants did not necessarily have better security habits than those with a less technological backgound. With the study by Friedman et al. dating from 2002 and using only personal computers as the users' device for connecting to the internet, our results indicate that their conclusions are still valid 15 years later on mobile devices.

Similarly, the privacy stance of participants (measured by usage of privacy-enhancing tools used and actions taken in the past, depicted in Figure 5) did not have any significant influence on the number of unsecured Wi-Fi networks they connected to. This indicates that, while users are prepared to install or use privacy-enhancing tools in a one time set-it-and-forget-it manner, they often lack the time or inclination to be continually aware about the security risks of using public Wi-Fi networks. This is in line with results from Dourish et al. [22] and Klasnja et al. [6] (studies from 2004 and 2009, respectively), where it is discussed that task-oriented users do not generally think about these issues when they are going about their work. Instead, they choose to delegate responsibility for security to tools, other individuals or institutions.

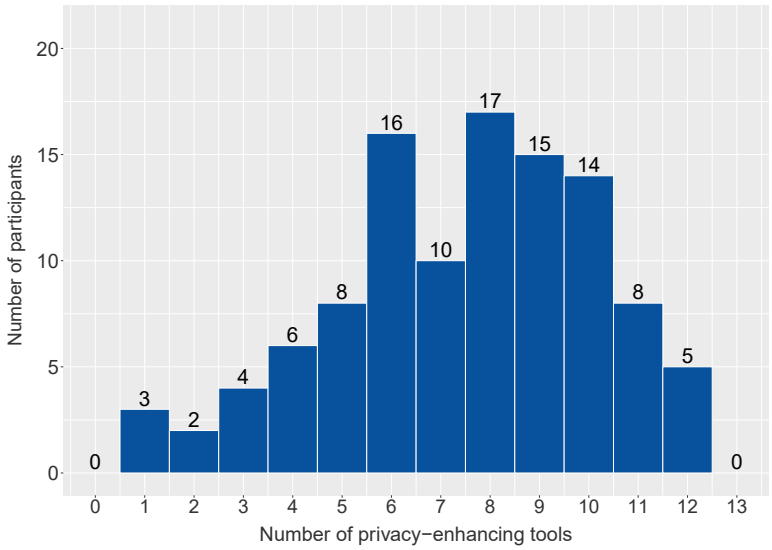

Figure 5. Number of privacy-enhancing tools and methods used by participants of the study. The majority of participants (53.70%) had used between six and nine of these tools and methods in the past.

This mismatch in privacy stance and security behavior directly translates to participants' perceptions about transmitted data: when confronted with specific scenarios about unencrypted connections that occurred on insecure networks (presented as a hypothetical scenario), 91% of participants indicated being worried about the corresponding data being available to eavesdroppers. Furthermore, participants are most concerned about the privacy of actual app data, even more so than they are about the privacy about the app's password. This result seems to confirm the Privacy Paradox, as participants are transmitting a significantly larger amount of data over insecure channels than they intend to.

It would be interesting to see whether the types of apps that are used in more insecure scenarios handle less privacy-sensitive data than those used in high-security scenarios. We did not explicitly label apps in our dataset as having access to "privacy-sensitive" data, as doing so would be inherently subjective, depending on for example the cultural background of the researchers. While the privacy sensitivity of the data itself was not the focus of this research, we consider it an interesting area for future work to use the permission accesses granted to apps as a proxy for the data they are able to access. This would allow for investigating possible correlations between the amount of sensitive data an app handles, and the security of the app's connections.

Asking the participants about their privacy-sensitiveness to the different types of information that could be transmitted by an app beforehand pushed them to think about what this data could comprise before answering questions about network owners or eavesdroppers having access to this data. Together with the previous results, this demonstrates that using very specific, personalized scenarios (instead of more general ones) might prove to work better to inform mobile device users about security and privacy issues.

7. Recommendations

The findings from the previous section lead to some recommendations for actions that can be taken by different stakeholders. These recommendations are laid out in this section, differentiating between three groups: recommendations for network providers, developers, and users are discussed in the following subsections.

7.1. Network Providers and ISPs

The fact that over one third of Wi-Fi networks participants connected to did not have any security enabled shows that even in 2017 more attention needs to go to pushing network operators to secure their Wi-Fi networks. As mentioned in the previous section, the biggest offenders are commercial entities and ISP hotspots. While convincing all commercial entities to upgrade their networks to provide security might prove difficult, convincing a few ISPs to do the same will yield an almost equally good result. Moreover, as these ISP hotspots are widely distributed (with each network name corresponding to a large number of individual access points), devices will often automatically connect to one of those networks, posing a large security risk. Indeed, they account for over 94% of all connection pairs. Thus, we recommend ISPs to eliminate any insecure hotspots from their network, instead providing only encrypted hotspots to their customers. If this proves to be difficult, e.g., because the ISP also wants to provide internet access to non-subscribers through a captive portal, we recommend offering two separate wireless networks: a secured network for subscribers, and an insecure network that allows the use of a captive portal. In addition, we think implementing the 802.11u wireless roaming standard and Hotspot 2.0 (also known as Passpoint) could provide benefits in this regard.

One consequence of cellular data replacing (or supplementing) Wi-Fi for mobile device users is that trust shifts from the Wi-Fi network providers to the mobile network operators. This shifts trust from the Wi-Fi network provider to these operators (they are now the middle man between the user's device and the other endpoint), and gives them the same responsibilities: they need to make sure the network is upgraded to the latest generation so users are not susceptible to eavesdropping attacks. While LTE provides significant security advantages over older generations of networks, it is not immune to attacks [23]. Whereas, at the moment of writing these do not pose an immediate threat to users in the form of eavesdropping attacks, these could still enable an active attacker to force a victim's device into using 2G or 3G rather than LTE networks, which can, in turn, make it possible to mount 2G- or 3G-specific attacks.

7.2. Developers and Operating System Vendors

Having security between the mobile device and the network, preventing eavesdroppers from monitoring metadata about network connections, is only part of a complete solution. With most participants (71%) having a high concern of their data being available even to the network provider, app developers need to secure against all possible forms of man-in-the-middle attacks. In practice, this means making sure that all connections between the user's device and the app provider's servers are end-to-end encrypted, and that the libraries and implementations used to achieve this are secure and up-to-date (see [5]). We recommend using some form of certificate pinning, where the public key certificate of the other endpoint is already embedded in the app package instead of relying on the system's certificate chain to validate the other endpoint's key. As 12.92% of logged connections (excluding servers of advertisement agencies) were insecure, app developers in general have some room of improvement.

A specific recommendation can be made to distributors of the Android operating system, too: while the fact that Android's `/proc/net/tcp` and `/proc/net/tcp6` files are readable for every installed application greatly helped performing these experiments, they also pose a potential privacy risk to Android users. Indeed, our app was able to infer the connections made by all other apps on users' devices without requiring any special permissions, leading to users giving feedback akin to *"it's creepy what your app is able to see"*. Barring any technical limitations the authors are not aware of, we recommend restricting access to these files from apps, making them available only to the operating system itself.

7.3. Mobile Device Users and Researchers

As was already indicated in Section 6, users tend to use a set-and-forget approach when dealing with security and privacy issues, limiting their security awareness when trying to complete a task at hand. This makes that even generally privacy-aware users are often unaware about security issues at the moment they occur.

To cater to the set-and-forget approach, users need to be able to delegate their security approach to a tool, setting it up at a time that is convenient to them. Such a tool can take the form of for example the Wi-Fi Privacy Ticker [10], informing the user at the exact moment privacy-sensitive data is being transmitted by their device, and allowing them to prevent it if desired. As far as the authors are aware, such a tool is currently not available for mobile devices, and developing it could prove to be an interesting area for future work.

Another approach could be to have either a tool or the operating system handle possible insecure situations differently, modifying the user interface to nudge users into making good security decisions as described by Balebako et al. [24]. For example, the operating system could be modified to make it more difficult to connect to unsecured networks, either by making this option less accessible in the user interface or by having the user explicitly dismiss a warning about the dangers of connecting to such a network (as is already the case on some operating systems). Similarly, unsecured networks could be prevented from being included in the list of "preferred networks" the mobile device will connect to automatically, still allowing the user to complete their task (by allowing a connection to an insecure network when needed), but preventing the device from connecting to a similar network later on. This is similar to the approach taken by the "Wi-Fi PrivacyPolice" tool [25], which can be set up to only allow connections to access points that were encountered before.

Virtual private network (VPN) services allow users to route all their network traffic through an intermediate server in an encrypted fashion, and are often touted as a solution to network security issues. While these services are indeed able to prevent an eavesdropper (or the network owner) from intercepting traffic, they present some other challenges. First, VPN services can be difficult to use for technically less educated users or users depending on services that actively block the use of a VPN. Second, and more importantly, VPN services are difficult to vet, with a recent study showing that 75% of Android VPN apps contain a third-party tracking library, and over 38% of them contain some type of malware [26].

8. Conclusions

In this work, we sought to understand mobile users' privacy and security assumptions when connecting to Wi-Fi networks. For this purpose, we conducted a study with 108 participants, monitoring the Wi-Fi networks they connected to and the connections made by apps on their device for a period of 30 days. After the monitoring phase, we asked them a number of questions about the gathered data, polling for both awareness and privacy sensitiveness on the data that was sent. With this, we assessed to what extent their privacy and security stances corresponded with actual security behavior.

Despite the trend of mobile users using cellular data for internet access, our results show that even in 2017 usage of Wi-Fi networks is very popular. There is even a noticeable increase in Wi-Fi popularity compared to 2009, with users on average connecting to 8 different Wi-Fi networks in a 30-day period. Over one third of these networks, and 13% of connections made by apps on user's devices are insecure, which poses a major security risk to the average mobile device user.

We show that, even though participants with a higher expertise in computer networks are more likely to be aware about the connections made by apps on their device, this does not translate to better security practices. Similarly, the usage of privacy enhancing technologies (such as a browser plugin providing tracking protection) in the past does not have a significant impact on security behavior on Wi-Fi networks. This confirms previous studies which state that users are inclined to see security as

a set-it-and-forget-it problem, where they delegate security to a tool or a different entity, not thinking about it when trying to accomplish a specific task later on.

This is a problem that is acknowledged by our participants: for 91% of data that was found to be transmitted in an insecure fashion on their devices, participants indicated they were worried about eavesdroppers being able to view this data. We confirm the Privacy Paradox by showing that participants are transmitting a significantly larger amount of data over insecure channels than they intend to.

We provided recommendations to network providers, developers and users to further enhance privacy and security for mobile device users. Furthermore, we expect that there are large benefits in using very specific, personalized scenarios to inform mobile device users about security and privacy issues.

Author Contributions: Bram Bonné designed the methodology and survey questions, wrote the monitoring and surveying software, analyzed the results, and wrote the paper; Gustavo Rovelo helped design the survey questions, performed the statistical analysis on the data, and helped write the paper; Peter Quax and Wim Lamotte helped design the methodology and survey questions, helped with the recruiting process and helped write the paper.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Appendix A. Recruitment Survey Questions

Disclaimer: the questions listed below are direct translations of the actual questions in Dutch, and may vary slightly in wording because of this translation.

Q1: Do you own an Android device which you use outside of your own home?
Options: Yes, No

Q2: Did you ever change the settings of your home network? e.g., the Wi-Fi password or the name of the network
Options: Yes, No, Don't know

Q3: Would you be able to explain what WEP, WPA and WPA2 are?
Options: Yes, No

Q4: If yes on the previous question, please explain what WEP, WPA and WPA2 are.
Open text response

Q5: How would you rate your own expertise in computer networks?
Options: Very high, High, Average, Low, Very low

Q6: What is your gender?
Options: Male, Female

Q7: What is your birth year?
Open text response

Q8: What is your highest earned degree?
Options: None, Elementary school, Lower part of high school, High school, Bachelor, Master

Appendix B. Exit Survey Questions

Disclaimer: the questions listed below are direct translations of the actual questions in Dutch, and may vary slightly in wording because of this translation.

For each survey, three Wi-Fi networks that the user connected to are chosen at most. For each network, at most three apps are chosen for which the participant is surveyed.

Appendix B.1. Introductory Questions

Q1-3: Within the context of app <app name>, how concerned are you about the privacy of the following data?

- Username
- Password
- Data (messages, information within the app, pages visited from the app, ...)

Options (for each of the different data types): Not at all concerned, Slightly concerned, Somewhat concerned, Moderately concerned, Extremely concerned

This question is asked for at most three apps that set up a network connection per Wi-Fi network, for a total at most three Wi-Fi networks. This creates at most 27 $(3\ apps \times 3\ networks \times 3\ data\ types)$ questions, with the total often being much lower as questions for the same app are consolidated.

Q4: How would you estimate the security of your home Wi-Fi network?

Options: Very bad, Bad, Acceptable, Good, Very Good, Don't know/I don't have wireless internet at home

Appendix B.2. Network Questions

Help text: "On <connection time> your device was connected to the <network name> Wi-Fi network. You provided the following information about this network: <user response>."

Q5: In which of the following categories would you put the owner of network <network name>?

Options: Family (own home network), friend of family (someone else's home network), employer (own company network), other company (company network), public institution (city network, museum network, ...), commercial institution (restaurant or cafe network, supermarket network ...), roaming network of home internet provider (<examples of local ISPs>), other

Q6: To what extent do you agree with the following statement: "The owner of <network name> is permitted to see all information (see previous page) of app <app name>"

Options: Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly agree

Q7: To what extent do you agree with the following statement: "A random person in the neighborhood of <network name> (e.g., someone standing on the street close to the building) is permitted to see all information (see previous page) of app <app name>"

Options: Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly agree

This question is only surfaced if the network is not secured with WEP, WPA, WPA2 or WPA-enterprise, *and* if the app is using unencrypted connections.

Q8: How likely would you say that the app <app name> actually sent data over the <network name> network?

Options: Extremely unlikely, Unlikely, Neutral, Likely, Extremely likely

Q9: How would you rate the security of the <network name> network?

Options: Much less secure than my home network, Less secure than my home network, as secure as my home network, More secure than my home network, Much more secure than my home network

Q10: To what extent do you agree with the following statement: "I trust the owner of <network name>"
Options: Strongly disagree, Disagree, Neither agree or disagree, Agree, Strongly agree

Appendix B.3. General Questions

Q11-23: While using the internet, have you ever done any of the following things?
Both this question wording and the relevant tools and options from [19] are used. These tools and options are:

- Used a temporary username or email address
- Added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger
- Given inaccurate or misleading information about yourself
- Set your browser to disable or turn off cookies
- Cleared cookies and browser history
- Used a service that allows you to browse the Web anonymously, such as a proxy server, Tor software, or a virtual personal network (VPN)
- Encrypted your phone calls, text messages or email
- Decided not to use a website because they asked for your real name
- Deleted or edited something you posted in the past
- Asked someone to remove something that was posted about you online
- Used a public computer to browse anonymously
- Used a search engine that doesn't keep track of your search history
- Refused to provide information about yourself that wasn't relevant to the transaction

Options: Yes, No, Not applicable to me, Don't know

Q24: Do you think that people should have the ability to use the internet completely anonymously for certain kinds of online activities?
This question is derived directly from [19].
Options: Yes, No, Don't know

Appendix B.4. Connection Awareness Questions

Q25: The app <app name> has effectively been sending data over the network <network name>. Were you aware of this happening?
Options: Yes, No

Appendix B.5. Feedback Question

Q26: Comments? Questions? Did we miss something? Let us know!
Open text response

References

1. Eurostat. ICT Usage in Households and by Individuals. 2016. Available online: http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database (accessed on 27 April 2017).
2. Poushter, J. *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*; Pew Research Center: Washington, DC, USA, 2016.
3. Bonné, B.; Quax, P.; Lamotte, W. Your mobile phone is a traitor!—Raising awareness on ubiquitous privacy issues with SASQUATCH. *Int. J. Inf. Technol. Secur.* **2014**, *6*, 393–422.
4. Troianovski, A. Phone Firms Sell Data on Customers. 2013. Available online: http://www.wsj.com/articles/SB10001424127887323463704578497153556847658 (accessed on 22 June 2017).
5. Georgiev, M.; Iyengar, S.; Jana, S.; Anubhai, R.; Boneh, D.; Shmatikov, V. The Most Dangerous Code in the World: Validating SSL Certificates in Non-browser Software. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), Raleigh, NC, USA, 16–18 October 2012; ACM: New York, NY, USA, 2012; pp. 38–49.

6. Klasnja, P.; Consolvo, S.; Jung, J.; Greenstein, B.M.; LeGrand, L.; Powledge, P.; Wetherall, D. "When I am on Wi-Fi, I am fearless": Privacy concerns & practices in everyday Wi-Fi use. In Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI '09), Boston, MA, USA, 4–9 April 2009; ACM Press: New York, NY, USA, 2009; p. 1993.
7. Norberg, P.A.; Horne, D.R.; Horne, D.A. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126.
8. Yee, K.P. User interaction design for secure systems. In Proceedings of the International Conference on Information and Communications Security (ICICS '02), Singapore, 9–12 December 2002; Springer: Berlin, Germany, 2002; pp. 278–290.
9. Lella, A.; Lipsman, A. 2016 U.S. Cross-Platform Future in Focus. Available online: https://www.comscore.com/Insights/Presentations-and-Whitepapers/2016/2016-US-Cross-Platform-Future-in-Focush (accessed on 27 April 2017).
10. Consolvo, S.; Jung, J.; Greenstein, B.; Powledge, P.; Maganis, G.; Avrahami, D. 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, Copenhagen, Denmark, 26–29 September 2010; ACM: New York, NY, USA, 2010; pp. 321–330.
11. Swanson, C.; Urner, R.; Lank, E. Naïve security in a Wi-Fi world. In Proceedings of the IFIP International Conference on Trust Management, Morioka, Japan, 16–18 June 2010; Springer: Berlin, Germany, 2010; pp. 32–47.
12. Kang, R.; Dabbish, L.; Fruchter, N.; Kiesler, S. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS '15), Ottawa, ON, Canada, 22–24 July 2015; pp. 39–52.
13. Chin, E.; Felt, A.P.; Sekar, V.; Wagner, D. Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12), Washington, DC, USA, 11–13 July 2012; ACM: New York, NY, USA, 2012; p. 1.
14. Clark, J.W.; Snyder, P.; McCoy, D.; Kanich, C. I Saw Images I Didn't Even Know I Had: Understanding User Perceptions of Cloud Storage Privacy. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; ACM: New York, NY, USA, 2015; pp. 1641–1644.
15. Tews, E.; Beck, M. Practical Attacks Against WEP and WPA. In Proceedings of the Second ACM Conference on Wireless Network Security (WiSec '09), Zurich, Switzerland, 16–19 March 2009; ACM: New York, NY, USA, 2009; pp. 79–86.
16. Schuermann, D.; Kicelo AdAway Hosts File. 2017. Available online: https://adaway.org/hosts.txt (accessed on 27 April 2017).
17. Google Play. Top Communication Apps. Available online: https://play.google.com/store/apps/category/COMMUNICATION/collection/topselling_free (accessed on 27 April 2017).
18. Dainotti, A.; Gargiulo, F.; Kuncheva, L.I.; Pescapè, A.; Sansone, C. Identification of traffic flows hiding behind TCP port 80. In Proceedings of the 2010 IEEE International Conference on Communications (ICC), Capetown, South Africa, 23–27 May 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–6.
19. Pew Research Center. Pew Research Center's Internet Project/GFK Privacy Panel Survey #2 Topline. 2014. Available online: http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_Topline_FINAL.pdf (accessed on 27 April 2017).
20. Roth, V.; Polak, W.; Rieffel, E.; Turner, T. Simple and Effective Defense against Evil Twin Access Points. In Proceedings of the First ACM Conference on Wireless Network Security (WiSec '08), Alexandria, VA, USA, 31 March–2 April 2008; ACM: New York, NY, USA, 2008; pp. 220–235.
21. Friedman, B.; Hurley, D.; Howe, D.C.; Felten, E.; Nissenbaum, H. Users' conceptions of web security: A comparative study. In Proceedings of the CHI'02 Extended Abstracts on Human Factors in Computing Systems, Minneapolis, MN, USA, 20–25 April 2002; ACM: New York, NY, USA, 2002; pp. 746–747,
22. Dourish, P.; Grinter, E.; Delgado de la Flor, J.; Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Pers. Ubiquitous Comput.* **2004**, *8*, 391–401.
23. Shaik, A.; Seifert, J.; Borgaonkar, R.; Asokan, N.; Niemi, V. Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. In Proceedings of the 23nd Annual Network and Distributed System Security Symposium (NDSS 2016), San Diego, CA, USA, 21–24 February 2016.

24. Balebako, R.; Leon, P.G.; Almuhimedi, H.; Kelley, P.G.; Mugan, J.; Acquisti, A.; Cranor, L.F.; Sadeh, N. Nudging users towards privacy on mobile devices. In Proceedings of the CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion, Vancouver, BC, Canada, 7–12 May 2011.
25. Bonné, B.; Lamotte, W.; Quax, P.; Luyten, K. Raising Awareness on Smartphone Privacy Issues with SASQUATCH, and solving them with PrivacyPolice. In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, London, UK, 2–5 December 2014; Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST): Ghent, Belgium, 2014; pp. 379–381.
26. Ikram, M.; Vallina-Rodriguez, N.; Seneviratne, S.; Kaafar, M.A.; Paxson, V. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In Proceedings of the 2016 ACM Internet Measurement Conference, Santa Monica, CA, USA, 14–16 November 2016; ACM: New York, NY, USA, 2016; pp. 349–364.