"*Free WiFi is not ultimately free*": Privacy Perceptions of Users in the US regarding City-wide WiFi Services

Prianka Mandal
William & Mary
pmandal@wm.edu

Tu Le
University of California, Irvine
tul10@uci.edu

Amit Seal Ami
William & Mary
aami@wm.edu

Yuan Tian
University of California, Los Angeles
yuant@ucla.edu

Adwait Nadkarni
William & Mary
apnadkarni@wm.edu

Abstract

City-wide free WiFi is one of the most common initiatives of smart city infrastructures. While city-wide free WiFi services are not subject to privacy-focused regulations and appeal to a broader demographic, how users perceive privacy in such services is unknown. This study explores perspectives of users in the United States regarding the privacy practices of such services as well as their expectations. We conducted surveys with 199 participants of US, consisting of those who had used such services (i.e., experienced users, n=99) and those who had not (i.e., potential users, n=100), assessing their satisfaction with the services, perceptions regarding data privacy practices of city-wide free WiFi services, and general expectations of privacy. We identify 14 key findings by analyzing the responses from participants. We found that participants are aware of the data collection and data sharing by the WiFi services and are uncomfortable with both but are still inclined to use the services as the need for WiFi outweighs privacy, as well as because of the significant *trust* they place in the services due to their non-profit and government-run nature. Our analysis provides actionable takeaways for researchers and practitioners, arguing for long-term privacy gains through a regulatory approach that treats city-wide WiFi as a utility, given the trust consumers place in it, and the overall tendency of consumers to trade-off privacy for WiFi access in this context.

Keywords

privacy, user perception, user expectation, wifi services, smart city

1 Introduction

With growing technology and urbanization, cities all over the world are being transformed into smart cities by providing public safety, a healthy environment, public transport, and many other facilities. One of the core smart city initiatives is providing city-wide free WiFi in public places. For instance, New York City launched the LinkNYC [2] WiFi service aimed at providing city-wide high-speed Internet *for free*. Similarly, Boston City introduced a public WiFi network, Wicked Free Wi-Fi [8], for people to get *free WiFi access* to find City services or browse the internet. While prior work [10, 17, 31] has explored the security and privacy implications of publicly available WiFi access (e.g., Starbucks WiFi), city-wide free WiFi services offer us a unique privacy context: where a publicly-owned, non-profit, entity (e.g., a city government) provides WiFi throughout a broad geographic area.

This context is important for three key reasons. First, while privacy-focused regulations such as the California Privacy Rights Act (CPRA) [6] allow users to assert rights over how organizations collect and use their private data, it is important to note that city governments administering smart city WiFi infrastructures are exempt from such regulations, as they are 501(c)(3) non-profits. Second, city-wide free WiFi services cover larger areas and may attract more users than individual, private, establishments such as restaurants. Third, it is entirely possible that since city-wide WiFi is provided by government/public entities, and funded by taxpayers, users may perceive it akin to a public utility such as water, electricity, gas, and public infrastructure, which may have impact on their privacy expectations and perception. Thus, while these services are in their incipient stages and gaining traction, it is timely to define the right privacy controls for this unique context, which requires us to first understand how users perceive privacy in such services, i.e., what they know and expect in terms of privacy when using city-wide free WiFi.

Contributions: This paper explores user perceptions and expectations of privacy practices in the context of city-wide free WiFi, through a mixed-methods, survey-based study with 199 participants based in the US, guided by the following research questions:

RQ1: *How have users found their interactions and experiences with city-wide WiFi services?* City-wide free WiFi is an emerging deployment approach that is being adopted across the world for providing better services. City-wide WiFi services are being deployed worldover, but are in their incipient stages. As a result, we do not have sufficient insight into the user experience with using these services, and the pros/cons they may associate specifically with city-wide free WiFi services. This is particularly important if we are to understand how users weigh the privacy costs associated with city-wide free WiFi with the benefits, i.e., if users experience significant benefits, they may be more willing to forego privacy. Alternately, if the utility experienced is minimal, then we may not need to invest in privacy controls, as users may not use city-wide free WiFi in the first place.

Proceedings on Privacy Enhancing Technologies 2025(3), 527–544

https://doi.org/10.56553/popets-2025-0111

RQ2: *How do users perceive the current privacy practices in city-wide free WiFi services?* Due to their unprecedented scale of deployment, as well as their management by government entities, users may perceive privacy differently when it comes to city-wide free WiFi services. Alternately, participants may inherit perceptions of privacy from traditional WiFi services, which may not transfer accurately to the context of city-wide free WiFi, e.g., the enforceability of privacy policies with regulations such as CPRA. Thus, we seek to study how users perceive the privacy practices of city-wide free WiFi services regarding data collection, retention, and sharing, in order to motivate appropriate privacy controls.

RQ3: *How do users perceive privacy policies offered by city-wide free WiFi services?* We seek to understand past user experiences with privacy disclosures, their interest in reading them, as well as their ability to reason about complexity or ambiguity in disclosures.

RQ4: *What do users expect in the form of privacy from the city-wide free WiFi services?* We are interested in learning about what users expect from city-wide free WiFi services, particularly because government entities own them and city-wide free WiFi services can be held to a higher privacy standard since they are generally intended as a public service. Particularly, we seek to understand what users expect in terms of privacy disclosure, as well as the collection, retention, and sharing of personal data from WiFi use.

To answer these questions, we conducted a user survey with 199 participants, including both *experienced users* (n=99), i.e., those who used city-wide free WiFi services previously, and *potential users* (n=100), i.e., those who had not, but who may use city-wide free WiFi in the future. Moreover, our participants from both categories are demographically diverse and generally of a non-CS/IT background, i.e., 82.91% of participants do not have an education in, or work in, the field of computer science, computer engineering, or information technology. Our study identifies 14 key findings ($\mathcal{F}_1$ - $\mathcal{F}_{14}$) that demonstrate important trends and inform on prominent perceptions of user privacy in this new context of WiFi services operated by the city.

This work is broadly situated in the area of user privacy perceptions [9, 25, 33, 39, 42, 50, 56], but more closely related to more recent work on understanding the privacy implications of WiFi hotspots [10, 17, 35, 36]. However, the paper studies the privacy of WiFi *provided by smart cities** (i.e., the public sector), as opposed to *private hotspots* in stores/restaurants, and this context makes the analysis and findings both timely and novel. To elaborate, while prior work on WiFi hotspots focused on analyzing dynamic aspects of security and privacy, such as vulnerabilities in the public WiFi infrastructure, actual user behavior, or tracking by hotspots [10, 17, 35, 36], we focus on understanding users' privacy perceptions regarding city-wide free WiFi. For instance, we show that despite knowing that the city-wide free WiFi service may collect personal information ($\mathcal{F}_4$), participants are willing to trade off their privacy ($\mathcal{F}_6$) due to the cost-effectiveness, availability ($\mathcal{F}_2$), and more importantly, *their trust in the benign use of data in the city/public context* ($\mathcal{F}_{10}$). These latent perceptions regarding user privacy when *the WiFi service is offered by the city government* are a novel contribution of this work. Moreover, this paper also reveals the factors that motivate users to use such services ($\mathcal{F}_1$, $\mathcal{F}_2$).

Furthermore, our study explores key aspects of privacy perceptions not discussed in prior work related to privacy policies [25, 27, 40]. For instance, we observed that while many users can reason about complex statements in privacy policies ($\mathcal{F}_{12}$), they are dissuaded by their length ($\mathcal{F}_{11}$) and prefer short summaries instead ($\mathcal{F}_{14}$). That is, it provides key insight into how users weigh the privacy costs associated with city-wide free WiFi services against their benefit and motivate the development of simpler privacy labels [29] for such services as well, as they have been for consumer IoT products [22, 23]. This preference is closely tied to users wanting to connect to WiFi quickly and presents a novel takeaway in this unique context.

All these findings from this work are distinct from prior work, tightly coupled with the public context, and will foster a timely conversation among policymakers, service providers, and governments regarding privacy in this basic smart-city initiative. Therefore, in the light of our findings, we make recommendations towards treating city-wide free WiFi as a utility instead of a product/service, thereby motivating research in the direction of several regulatory protections that exist for protecting private data available to utilities [1, 3].

The remainder of this paper proceeds as follows. Section 2 presents a comparison with related work. We present the methodology of our user study in Section 3, and the results and findings in Section 4. We provide a detailed discussion along with recommendations in Section 5. Section 6 discusses the limitations of this paper. Section 7 provides concluding remarks.

2 Related Work

This work is the first to explore the privacy perceptions and expectations of user from city-wide free WiFi services, and is closely related to the following areas:

User perceptions of privacy: Recent work has explored privacy perceptions focusing on various platforms. In particular, Balash et al. [13] explored security and privacy perceptions regarding third-party API access to Google accounts. Mink et al. [42] analyzed user privacy concerns regarding fitness tracking apps, while Abrokwa et al. [9] investigated user perceptions regarding privacy on various smartphone and smart speaker platforms. Similarly, another line of research is conducted based on various populations and age groups, such as Hanson et al. [25]'s investigation of crowd workers' privacy perceptions regarding hyper-personalized advertising, Balash et al. [12]'s work on the security and privacy perceptions of students regarding online proctoring services, and Ray et al. [47]'s study of privacy perceptions among older adults. We contribute to this body of work by exploring user privacy perceptions in a unique domain: free WiFi services in smart cities. We show results and insights that improve our collective understanding of privacy perceptions of critical and necessary public WiFi services.

Smart city security and privacy: With the recent growth in smart city initiatives [19, 32, 43, 52], the research community has started to focus on the security and privacy implications of smart cities [14, 21, 28, 33, 39, 45, 50, 55]. For instance, Zhang et al. [55] described security and privacy challenges in various smart city applications, considering various aspects (e.g., energy, environment, industry, living, and services) and the technical architecture (e.g., sensing components, heterogeneous network infrastructure, processing units, and control and operating components). Similarly,

Braun et al. [14] discussed privacy threats in terms of data mining, sharing, integration, and mashups, as well as cloud security. Moreover, Martinez-Balleste et al. [39] defined the citizens' privacy needs in smart cities, whereas Peters et al. [45] proposed a privacy awareness framework that helps users to make data-sharing decisions. Furthermore, prior work has experimentally demonstrated and studied security and privacy issues in smart cities, such as Li [34] et al.'s study of data over-collection in smart cities, and Farahat et al. [24]'s work on protecting data secrecy by securing the WiFi-based data transmission system. A key difference in our paper is that while prior work focuses on security and privacy problems in smart city applications, we focus uniquely on privacy perceptions of city-wide free WiFi services, which is still unexplored and is one of the core initiatives of smart cities.

In terms of the goal of broadly understanding privacy perceptions in smart cities, the work of Stahlbrost et al. [50] is closest to our paper, as it explored citizens' perspectives on privacy issues related to audio monitoring in the smart city. However, our chosen smart city application of city-wide WiFi is not only different but also significantly more prevalent and impactful. Moreover, our study explores several important aspects of privacy perceptions that were not discussed in prior work, such as users' awareness of data collection, their desire for privacy-related information, and their ability to reason about complex statements from privacy policies, to name a few, leading to 14 unique findings.

Security and privacy analysis of WiFi hotspots: Since the availability of public WiFi hotspots is increasing significantly [51, 53], there has been significant research focusing on security vulnerabilities in public WiFi [10, 17, 35–37, 54]. For instance, Cheng et al. focused on understanding the data leakage from WiFi hotspots by analyzing packets of users from 15 different airports [17], whereas Lotfy et al. examined the types of web links users browse using public WiFi, and their awareness of it [35]. On the other hand, Ali et al. performed a privacy analysis of 67 unique public WiFi to analyze tracking behaviors and privacy leakage [10]. Moreover, prior work has explored user behavior when using public WiFi, with Choi et al. analyzing risky behavior [18], and Maimon et al. analyzing self-protective behaviors [36, 37]. The prior work mostly focused on analyzing dynamic aspects of security and privacy, such as vulnerabilities in the public WiFi infrastructure, actual user behavior, or tracking by hotspots. Our study of user perceptions of privacy regarding public WiFi is related but different in scope from prior work. In particular, we identify latent patterns in how users perceive their privacy in this domain, in terms of their knowledge and comfort regarding how their data is collected, shared, and stored, as well as their perspectives on privacy disclosures. Another key difference is that we study the privacy of high-speed free WiFi services provided by smart cities for the citizens, which are different from the WiFi services provided by stores or restaurants.

Finally, our work, particularly some of the findings, are broadly related to prior work on obtaining informed consent from users using appropriate privacy disclosures and approaches that express privacy policies in accessible forms, such as privacy nutrition labels [22, 29, 30]. Unique to our study, we demonstrate that participants can reason about complex, ambiguous statements from privacy policies ($\mathcal{F}_{12}$). Furthermore, we qualitatively analyzed comments from participants and observed that instead of the complexity, the main hurdle in obtaining informed consent, in the unique context of smart cities, is the length and verbosity of the privacy policy documents ($\mathcal{F}_{11}$), while generally preferring short summaries instead ($\mathcal{F}_{14}$). Moreover, we find that disclosure is, to a certain extent, moot in a smart city context, as participants are willing to use the services regardless of the impact on privacy, which motivates our recommendation for regulatory protections regardless of consent.

3 Methodology

To explore the user perspective on city-wide free WiFi services privacy practices, we conducted a two-phase study, composed of a preparatory survey followed by an in-depth, detailed survey with 199 participants recruited through Prolific. In this section, we provide a brief overview of the survey preparatory study, a summary of the survey design, participant recruitment, and ethical considerations.

3.1 Preparatory study

We first conducted a preparatory survey aimed at getting an initial understanding of the user perspectives on the city-wide free WiFi services. This section provides a brief overview of the preparatory survey.

We recruited participants from our local area through a discord server, which is a dedicated community of local Pokemon Go [4] players. Our rationale behind choosing this user population is that as players of an augmented reality game, they are active internet users who often use the internet on the go, especially in public places, and hence, would be much more likely to use city-wide WiFi services. This survey had Institutional Review Board approval, and all participants were compensated.

We obtained 58 valid responses from the local participants, of which 17 participants had previously used city-wide free WiFi services, and the remaining 41 had not used them yet. Among 17 participants who had used city-wide free WiFi, 11 participants expressed that they had satisfactory experience of using it. When asked about data collection, only a few (3/58) participants explicitly think that city-wide free WiFi services do not collect data from users. We also found that while most participants are not comfortable with data collection (34/58) and data retention (46/58), they also showed interest in using these city-wide free WiFi services, as one participant defined these services as *"helpful but creepy"*.

These observations guided us to investigate through broader perspectives. Therefore, we conducted our study with 199 participants and asked them to provide more clarifications.

3.2 Survey Design

As shown in Figure 1, our survey included several sections focusing on different aspects of privacy practices of smart-city WiFi, such as data collection, data retention, data sharing, and privacy policies of city-wide WiFi services, and we asked questions regarding participants' perspective on those aspects. While designing the survey, we aimed to draft straightforward questions for our target expert population based on established privacy research literature [11, 21, 25, 27, 33, 38, 46], the authors' past experience in such research, and the feedback from our preparatory study. The

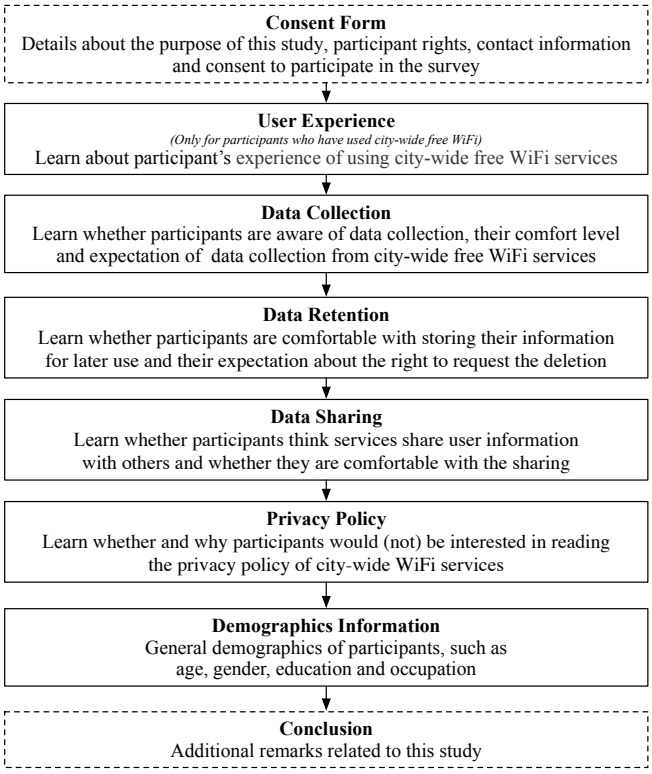

Figure 1: Overview of the survey design.

summary of those sections is as follows, with the details released on Appendix A.

(1) **User Experience:** This section was only presented to participants who explicitly indicated to be experienced with using city-wide free WiFi services. Participants were asked to share their experience of using the service(s). Particularly, we asked participants where they used the service, for how long, and their level of satisfaction with it. We also asked all participants whether they would check the compatibility of their device before using the service, given that certain providers such as LinkNYC (implicitly) offer a secure connection to compatible devices only.

(2) **Data Collection:** Participants were asked about their perspective on data collection practices by city-wide WiFi services. We asked participants whether they believed such services collected personal information from users, the types of information they thought such services collected, and whether they were comfortable about their data being collected. We further asked whether participants were comfortable with the service requiring their email address to offer services and determine their location. Finally, we asked about participants' expectations regarding their right to know about personal information collected by service(s).

(3) **Data Retention/Storage**: We asked participants about their perspectives on data storage/retention by city-wide free WiFi services. The goal was to understand whether they were comfortable with the service storing their information for later use. We also asked users to provide an estimate for how long they would be comfortable with when it comes to data retention. We then asked participants to provide their opinions regarding having the right to request the deletion of their information.

(4) **Data Sharing**: Participants were asked about their perspectives on information sharing of the WiFi services. We asked participants whether they believed or assumed that services shared user information with others and whether they were comfortable with it. We further asked participants about the types of information they thought the services shared with third parties, the types of information that should be allowed to be shared, and the types of third parties that should be allowed to obtain the shared information.

(5) **Privacy Policy**: Finally, we asked only those participants who have experience of using city-wide WiFi services whether they had read privacy policies before using the services in the past. Further, we asked all participants whether they were interested in reading the privacy policy and why they were interested. We collected a few ambiguous statements from a popular city-wide free WiFi service, LinkNYC [2], about collecting location and browsing history and asked participants to identify relationships among these statements.

(6) **Demographic Information**: We asked participants to provide basic demographic information such as age, gender, education, and occupation.

Before releasing our survey to the intended participants, we conducted pilot testing with four graduate students and revised the survey based on the feedback until no issues were raised. The pilot testing data were excluded from our analysis to avoid biases.

Table 1: Participant Demographic Information

		$users_{exp}$ (n=99)	$users_{potn}$ (n=100)
Gender	Male	39	28
	Female	58	69
	Non-binary	2	2
	Other	0	1
Age	18-29 years old	50	51
	30-49 years old	44	47
	50-64 years old	5	2
Education	Less than high school	1	0
	High school graduate	9	18
	Some college	22	29
	2 year degree	12	7
	4 year degree	36	36
	Professional degree	3	1
	Doctorate	1	0
	Masters	15	9
IT Experience	Have an education in, or work in , the field of computer science, computer engineering, or IT	17	11
	Do not have an education in, or work in , the field of computer science, computer engineering, or IT	79	86
	Prefer not to answer	3	3

3.3 Participant Recruitment

We recruited participants from Prolific[1] at two stages. First, we conducted a screening survey to recruit two types of participants:

[1]https://www.prolific.com

experienced users ($users_{exp}$), i.e., those who had used city-wide WiFi services previously, and *potential users* ($users_{potn}$), i.e., those who had not yet. Note that designating a participant as a potential user simply indicates the lack of usage prior to the survey and does not mean that they would not use smart city WiFi services in the future. In fact, they are potential users given the proliferation of city-wide WiFi services, and they have certainly expressed interest, as seen in their responses.

We did not seek to balance the number of participants by demographic criteria, for two key reasons. First, given our focus on understanding the perspectives of both experienced and potential users, our recruitment criteria focused on the participants' experience with city-wide free WiFi, in order to recruit a balanced number of responses from both experienced and potential users. Second, given that the demographic distribution of the *target population* of city-wide WiFi services is unknown, it is unclear if balancing across all demographics would translate into a representative sample (e.g., if the target population is in practice imbalanced/skewed toward people below age 49, or women, then a balanced sample would *not* be representative).

Thus, instead of balancing demographics, we choose to sample based on usage experience. To elaborate, via the screening survey, we first asked participants whether they had ever used city-wide free WiFi services, and received 707 responses. We invited these 707 participants (consisting of both experienced and potential users) to participate in the survey, and stopped the survey after receiving 100 complete responses from each type. Note that we decided to stop at 100 responses of each type as this sample size is comparable to other similar studies published in the privacy venues [12, 47].

We obtained valid responses from 99 experienced users and 100 potential users. We compensated all of our participants who participated in the screening and/or main survey following the recommended rate given by Prolific that are based on survey completion time. We followed their rate of $10/hour, paying $3.00 to experienced users (18 minutes, longer survey with experience-related questions) and $2.50 to potential users (15 minutes, no experience questions).

Table 1 provides demographic information about our participants separated by potential and experienced samples. All of our participants are from the US, given our focus on this locale. Note that there are no significant differences in the demographic distributions between our experienced and potential users, and both populations show similar demographic trends. As we did not select participants based on demographic criteria during our recruitment, this lack of distinction is coincidental.

3.4 Coding and Analysis Method

We conducted descriptive statistical analysis to present the quantitative results. To analyze free-text responses from the survey, we used reflexive thematic analysis with an inductive coding approach [15]. First, two coders randomly selected a subset of the data (20-30%) per question to create the preliminary codebook. Next, the coders split the data and used the preliminary codebook to code the split data independently. Moreover, the authors held an agreement-disagreement discussion to reach a consensus for each coded response. We did not rely on inter-rater reliability as our goal was to capture the diverse perspectives and experiences from the responses irrespective of the number of times they appeared [41]. For any segment that could not be coded using existing codes, the authors repeated the above steps, i.e., went through a subset of unlabeled data to introduce new codes in the codebook. By analyzing the recurring codes, and analyzing the responses, we then determined the themes. We coded all the responses and iterated through the thematic analysis steps until no new themes emerged, and the themes were finalized. We present our results based on those themes in Section 4.

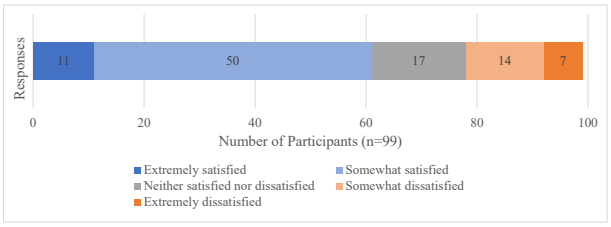

Figure 2: User satisfaction from city-wide free WiFi services

Table 2: The duration of using the city-wide free WiFi services, as reported by 99/199 participants who used city-wide WiFi previously.

Categories	Participants (n=99)	
	Count	Percentage
Less than a week	23	23.23%
More than a week but less than a month	6	6.06%
More than a month but Less than a year	18	18.18%
More than a year	16	16.16%
Occasionally	19	19.19%
Others	17	17.17%

3.5 Ethical Considerations

The study protocol was approved by our Institutional Review Board (IRB). We worked with our IRB to ensure ethical compliance. Participants were informed about the goal and logistics of the study before participating. They provided their consent to participate in the study through a consent form. Participation was voluntary, and withdrawal at any time was allowed without penalty. Participants were also informed that the information collected through the survey would be anonymized.

4 Results

This section describes the results from our analysis of the survey responses from 199 Prolific participants (denoted as **P1→P199**) where, participants **P1** to **P100** are $users_{potn}$ and participants **P101** to **P199** are $users_{exp}$.

4.1 Experience with Using WiFi: Much Needed Utility with Inconveniences

Of all our survey participants, 99/199 Prolific participants reported using city-wide WiFi services previously. When we asked participants to share their perspectives on the utility and experience of using WiFi (**RQ1**), two recurring themes came up frequently,

regardless of the background of the participants. First, of all the participants spread across 75 unique cities (see Appendix B for city names), more than half (61/99 or 61%) expressed that they were satisfied with the experience of using city-wide free WiFi as shown in Figure 2, irrespective of the duration they used the service for (from less than a week to more than a year, as shown in Table 2). Note that 14/99 participants mentioned having used city-wide free WiFi in more than one city; however, we collect and analyze their overall experience with such services, and the results do not associate satisfaction or experiences with individual cities (see Appendix B for a detailed explanation). These results indicate that city-wide free WiFi offers significant value to users, as aptly described by a user, **P104**, who found the service particularly useful in a remote location, i.e., *"...it was especially good since the town was located in the mountains."* (**P104**). We also found that the satisfaction level with city-wide free WiFi actually does not depend on the duration of the usage. For instance, participants who used the city-wide free WiFi for one week can be either satisfied because it *"it worked fine"* or dissatisfied because they found it to be *"very slow"*. Further, the satisfaction level does not depend on the geographic location; rather, it mostly depends on the usefulness of the city-wide free WiFi.

Despite the usefulness, nearly all participants shared that they experienced various issues related to the WiFi, such as slow and unreliable connection and spot-based connectivity issues, e.g., as **P158** mentioned, "*It was slow and had poor connection*".

However, regardless of the issues experienced, several participants explained that they were generally satisfied because "*... it gets the job done*" (**P159**), even if improvements are desired, e.g., as **P156** explained,

> "*I love having the option for free city WiFi, (but) I think the service could be improved.*"

Finding 1 ($\mathcal{F}_1$) – Participants generally focus on the utility of city-wide free WiFi regardless of the inconveniences they experience.

We further analyzed the open text responses to identify the motivating factors for using city-wide free WiFi, which we discuss next. The most common factor participants mentioned for using city-wide free WiFi was *its free nature*. In other words, participants, being cost-conscious, appreciated city-wide free WiFi as a service, as **P07** states,

> "*The fact that the Wi-Fi is free makes it very tempting to me!*"

Another factor that came from participants' responses is *its city-wide availability*. Participants shared that the city-wide free WiFi is a necessary utility, especially when traveling to places that are not covered by their cellular data connectivity networks. In other words, *users consider it as an alternative to cellular connectivity*. For example, **P116** shared that:

> "*... an excellent service when traveling out of the country where I didn't have cell service*"

Furthermore, a participant (**P111**) mentioned that *they won't use city-wide free WiFi as long as their cellular data connectivity is available*, which indicates their lack of trust in city-wide free WiFi. An

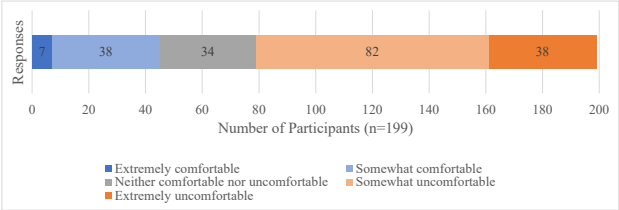

Figure 3: Participants' comfort regarding the collection of information by the city as a part of the WiFi service

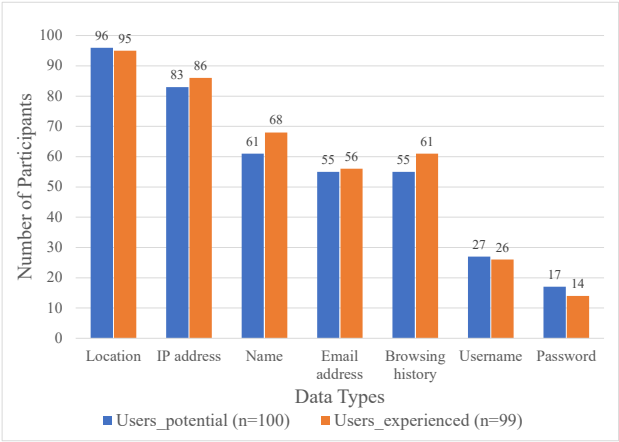

Figure 4: Types of personal data that survey participants believe to be collected by city-wide free WiFi

additional, indirectly related factor the participants mentioned is *the presence of VPN*. At least four participants were confident that using a VPN would protect their privacy and therefore were more willing to use city-wide free WiFi without worrying, as **P113** stated that,

> "*There are simple ways to protect from WiFi providers collecting data, such as a VPN.*"

Finding 2 ($\mathcal{F}_2$) – The motivating factors for using city-wide free WiFi are cost-effectiveness and availability, particularly in areas without cellular coverage.

4.2 User Perspectives – Understanding the Utility and Privacy Trade-off

This section seeks to answer **RQ2** by analyzing participants' perspectives on data collection, retention, and sharing by cities through their city-wide free WiFi services. Particularly, we focus on what participants believe occurs at present when city-wide free WiFi services collect their data, and seek to understand if the unique context of government operation impacts the perceptions.

4.2.1 Data Collection. More than half (53.77%) of participants ($users_{exp}$= 52, $users_{potn}$= 55) believe that city-wide free WiFi services collect personal information from users, whereas only 3.52% ($users_{exp}$= 5, $users_{potn}$= 2) think otherwise. The remaining 42.71%

($users_{exp}$= 42, $users_{potn}$= 43) participants were not sure about whether services collect data or not, irrespective of having prior experience of using (n=42) or not using (n=43) them.

Finding 3 ($\mathcal{F}_3$) – A negligible portion of participants (3.52%) were explicitly confident that city-wide free WiFi services do not collect personal information of users.

Next, we asked participants to identify the information that they think the services collect from a given list of private data types drawn from prior work (see the survey instrument in Appendix A). Almost all, i.e., 95.98% ($users_{exp}$= 95, $users_{potn}$= 96) participants indicated location, with the other popular choices being IP address ($users_{exp}$= 86, $users_{potn}$= 83), name ($users_{exp}$= 68, $users_{potn}$= 61), browsing history ($users_{exp}$= 61, $users_{potn}$= 55), email address ($users_{exp}$= 56, $users_{potn}$= 55), username ($users_{exp}$= 26, $users_{potn}$= 27), and password ($users_{exp}$= 14, $users_{potn}$= 17). Figure 4 shows a breakdown of the personal data types in terms of the percentage of $users_{exp}$ and $users_{potn}$ who believe that city-wide WiFi services collect them. As shown in the figure, experience played no significant role when it came to perceiving data collection: the distribution of participants, regardless of prior experience, was roughly the same when it came to believing in the occurrence or absence of data collection.

Finding 4 ($\mathcal{F}_4$) – Majority of participants, i.e., over 61%, believe that city-wide free WiFi services collect their personal information, such as location, IP Address, and name.

Further, we found that 60.30% ($users_{exp}$= 55, $users_{potn}$= 65) participants are not comfortable with the perceived data collection practices by city-wide free WiFi, as shown in Figure 3, expressing that it is *... violation of privacy (***P54***)*. Overall, participants expressed concern regarding data collection by the city, owing to the lack of disclosure, and general concerns regarding usage/sharing, i.e., as stated by **P46**:

> "*It has become harder to protect personal information and even to know when it is being collected. I would be concerned about what information was being collected and how it was being used.*"

Participants also cited concerns regarding collection because they perceived that there was no real need to collect it, as **P42** aptly states:

> "*I don't see a reason why the city would need access to my personal information.* "

Furthermore, participants emphasized that since the service is provided by a city, i.e., a public, non-profit enterprise, they *expect the city to not mine data for profit*, as shared by **P85**:

> "*It should be a free service to help the community. Not an opportunistic moment to mine data from unwitting citizens.*"

Finding 5 ($\mathcal{F}_5$) – Participants are uncomfortable with the collection of private data by city-wide free WiFi services. The most common reason cited is the perceived lack of need for data collection in the WiFi context, *particularly by a non-profit, government entity.*

In contrast, we find that for some specific types of data, such as location and email address, participants were okay with collecting them in lieu of using the city-wide free WiFi. As **P104** states,

> "*I am not someone who is really concerned about them knowing my email or location. I am not trying to hide.*"

More specifically, when we asked participants about how comfortable they are with city-wide free WiFi services requiring their email address, about half of participants i.e., 53.27%, ($users_{exp}$= 54, $users_{potn}$= 52) were comfortable with it, whereas 32.17% ($users_{exp}$= 30, $users_{potn}$= 34) were uncomfortable and 14.57% ($users_{exp}$= 15, $users_{potn}$= 14) were neutral about it. Furthermore, one common reason for being comfortable with data collection is that the participants believe the city needs to collect such types of data for the purpose of providing better city-wide free WiFi, thus being comfortable with data collection practices. As **P136** mentioned:

> "*That's pretty basic information just to help give a better connection*"

Lastly, some participants stated that *nothing is free*, expressing that they consider it as a trade-off for getting the service for free. That is, when they choose to use city-wide free WiFi, they are agreeing to let such services collect data, as **P166** states, *"you either pay for the product or you are the product"*. Similarly, **P108** provided an elaborate response regarding the trade-off:

> "*I utilize public wifi networks for their convenience, fully aware that the trade-off is that any and all data related to my usage of that network may be collected or monitored. I accept the breach of privacy because there are valid reasons for it...*"

Finding 6 ($\mathcal{F}_6$) – Participants are generally ready to trade off privacy, i.e., tolerate the (perceived) data collection by city-wide free WiFi services, if the data contributes to an improvement in service. Some participants take it a step further, and are willing to forego privacy entirely in lieu of the *free* service.

Prior research has observed a similar sentiment among users, i.e., that users are aware that service providers collect data, and comfortable with the collection if the data is used to improve the service [27].

4.2.2 Data Retention and Sharing. As we discussed, most participants were not comfortable about the city collecting information through city-wide free WiFi. Unsurprisingly, participants were not comfortable with data retention and sharing either.

When participants were asked about city-wide free WiFi storing their information for later use, 70.35% participants ($users_{exp}$= 65, $users_{potn}$= 75) were *somewhat or extremely* uncomfortable, whereas only 15.08% ($users_{exp}$= 19, $users_{potn}$= 11) were comfortable and 14.57% ($users_{exp}$= 15, $users_{potn}$= 14) were neutral about storing their information. In addition to this, when we asked participants about the duration for which they believe it is acceptable for the data to be stored, participants, in general, were not comfortable with long-term data retention. More specifically, 51.76% ($users_{exp}$= 50, $users_{potn}$= 53) participants expressed that a duration of at most one month was appropriate, whereas 34.17% ($users_{exp}$= 30, $users_{potn}$= 38) were unsure, 9.55% ($users_{exp}$= 11, $users_{potn}$= 8) chose at most 6

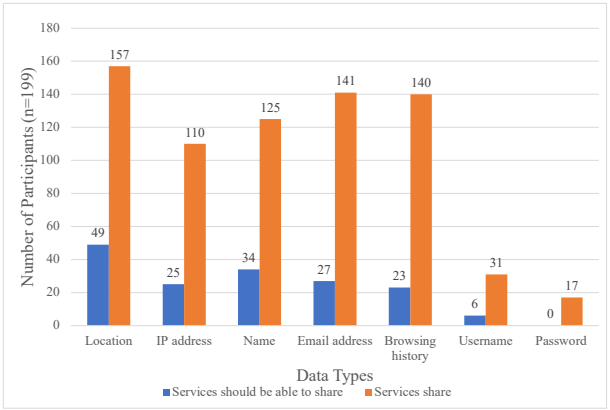

Figure 5: Comparison between what information city-wide free WiFi services share with third parties, as per participants, and what information they should be able to share

months, 4.02% ($users_{exp}$= 8, $users_{potn}$= 0) chose up to a year, and only one participant shared that the retention limit should be 5 years or longer.

Finding 7 ($\mathcal{F}_7$) – Participants are generally not comfortable with data retention. More than half of the participants believe that city-wide free WiFi services would not retain data for a long term, i.e., more than a month.

When participants were asked about data sharing, 59.8% ($users_{exp}$= 57, $users_{potn}$= 62) believed that services share information with third parties. In contrast, only 23.12% ($users_{exp}$= 24, $users_{potn}$= 22) participants think services do not share information with third parties, with an additional 34 participants being unsure. We not only asked participants about what data they believe city-wide WiFi services share with third parties, but also what data they believe should be shared, and summarized the responses in Figure 5. As seen in the figure, for most private data types, *while participants do believe services share the data in practice, very few believe that this sharing should continue.*

Finding 8 ($\mathcal{F}_8$) – Participants believe that personal information collected by city-wide free WiFi is generally shared with third parties, and express concern with the sharing of most kinds of private data.

In order to understand how users perceive the privacy-utility tradeoff, we asked participants if they would explicitly consent for city-wide free WiFi services to collect data, given their perceived notions of how their data would potentially be shared. About 35.18% ($users_{exp}$= 29, $users_{potn}$= 41) participants responded that they would not provide consent, after having considered what data these services share (according to their perception), generally citing the lack of transparency, as stated by **P143**:

> "*I would not want my information shared with third parties because I do not know what it will be used for.*"

At least five participants declined to consent to avoid advertisement and spam calls, i.e., as **P132** states,

> "*Personal data sharing snowballs so quickly into spam calls and emails, and I am sick of it.*"

Finding 9 ($\mathcal{F}_9$) – Participants would not consent to data collection if they knew it was being shared, due to the concern of privacy invasion, to avoid spam and advertising, and mainly because there was little transparency regarding how this data would be used by the third parties.

The fact that the WiFi service is offered by a government entity may have some bearing on why users would not consent to data being collected for sharing with advertisers. That is, this perception regarding city-wide free WiFi deviates from what prior work has found regarding data sharing and advertising in the the smart home, a commercial domain by nature, where users were generally comfortable with data being shared for advertising [56].

Further analysis shows that only a small portion of participants (19.6% or 39/199) believe that city-wide free WiFi services share user information with third parties, and would not provide consent to data collection as a result. That is, only these participants are genuinely concerned about their privacy and would not want to share their information with unknown parties. However, the rest of this section will show that participants trust the city regarding data sharing.

About 14.57% ($users_{exp}$= 17, $users_{potn}$= 12) participants mentioned that they would be okay with their information being collected and subsequently shared with third parties, mainly as they *trusted* the service, and believed the information would be used for benign reasons, as **P72** stated,

> "*... I don't think they would do anything too dishonorable since it is run by the city, so I see no reason not to use a viable service when it can't really hurt me.*"

More importantly, most, i.e., 50.25% ($users_{exp}$= 53, $users_{potn}$= 47) participants were ambivalent (i.e., indicated "maybe"), and stated that they would be open to (or against) sharing based on whom the data would be shared with and what it would be used for, or based on how much they needed WiFi at the moment, i.e., as **P64** states,

> "*I probably wouldn't, but it would also depend on how desperate I was to connect to the internet.*"

. In fact, approximately 32.16% participants mentioned that they may accept the trade-off depending on their *"need"*. A comment from **P53** aptly expresses this sentiment:

> "*I might decide in a moment of need that I need wifi more than I need privacy.*"

Furthermore, participants believe that sharing (or selling) their private data was acceptable consider privacy a viable trade-off for free WiFi, as stated by **P156**:

> "*Typically my need for wifi outweighs my need for privacy*"

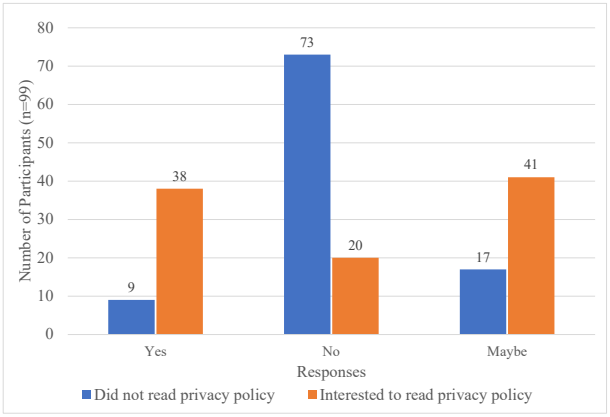

Figure 6: Participants' interest in reading privacy policy in comparison with not reading privacy policy. Note that these results are from those participants (n=99) who have used city-wide free WiFi previously.

Finding 10 ($\mathcal{F}_{10}$) – A significant minority of the participants (30%) would trade off privacy in the context of data sharing, i.e., consent to data collection even if they knew it was being shared with third parties. Common rationales include *trust in the city* for benign usage of the data, followed by a realization that their need for accessing WiFi for its utility may outweigh their need for privacy.

This observation complements prior work [25], which has found that users are likely used to the fact that sharing personal information is often an unavoidable aspect of accessing the Internet.

4.3 Perspectives on Privacy Policies

This section describes how participants perceive privacy policies in the context of city-wide free WiFi services (**RQ3**). We analyzed whether participants are interested in reading the privacy policy and why, as well as their understanding of privacy policy statements.

4.3.1 Likelihood of reading privacy policies. When participants were asked whether they would be interested in reading the privacy policy prior to using the service, 47.74% ($users_{exp}$= 38, $users_{potn}$= 57) participants responded in the affirmative, with an additional 35.68% ($users_{exp}$= 41, $users_{potn}$= 30) indicating that they may be interested, and only 16.58% ($users_{exp}$= 20, $users_{potn}$= 13) showing no interest. The most common rationale from participants showing interest was their motivation to know more about the use of their personal information. That is, as **P27** states:

> "*I would want to know how much of my personal and private information was going to be shared/sold with third parties and how confidential it would be kept.*"

Moreover, we found that participants also preferred to have the privacy policy available, regardless of reading. As **P14** mentioned:

> "*It's good to at least be offered information regarding privacy policy whether or not people read it thoroughly, and I would like that opportunity.*"

When asked about their experiences of reading privacy policies, 73.74% (73/99) of the users from the "$users_{exp}$" set reported not having read privacy policies prior to using city-wide free WiFi services in the past, with only 9.09% (9/99) indicating that they had, and the rest, i.e., 17.17% (17/99) indicating "maybe". However, a significant number of the same set of participants showed interest in reading the privacy policies, i.e., 38.38% (38/99) indicated that they were interested, 41.41% (41/99) indicated "maybe", whereas 20.2% or 20/99 indicated they were not. These numbers indicate that at least some of the participants who had not read privacy policies previously were interested in doing so (i.e., since only 9.09% had read policies previously, but 38.38% were interested in reading them), as illustrated in Figure 6.

This result raises an important question: *if many of the participants are interested in reading privacy policies, why had a majority not read them in the past?* Our analysis of participant comments revealed several reasons that caused them to refrain from reading the privacy policies. The most common reasons include reasons often reflected in prior work [40], such as the disclosure documents being long and verbose, being hard to understand, and requiring a long time to read. As **P46** states,

> "*The privacy policy is often long and full of jargon. It seems they are intentionally written that way so that people do not want to take the time to read and understand them before agreeing.*"

However, we also found that no matter how readable the privacy policy is, connecting to WiFi is perceived as a quick task, and reading a detailed privacy policy would not be desirable to most participants who simply want to connect and be on their way, as aptly stated by **P165**:

> "*No one has time to read those long forms just to use wifi quick*"

Finding 11 ($\mathcal{F}_{11}$) – Although participants are interested in reading privacy policies, they generally find the policy documents long, verbose, and full of jargon, which dissuades them from reading the policy prior to using the service.

This finding echoes prior work, e.g., McDonald et al. [40] discuss how users find reading privacy policies time-consuming, as our participants reported as well. However, a key difference is that a significant number of our participants showed interest in reading privacy policies, which deviates from the general notion expressed in literature that users do not want to read privacy policies. We further analyze participants responses and delve deeper into how participants would like to receive the information contained in their privacy policies, in order to match the pace required in connecting to a WiFi service, which we report in $\mathcal{F}_{14}$.

4.3.2 User assessment of complex privacy policy statements. To understand how participants perceive particularly ambiguous/complex statements from privacy policies of city-wide WiFi services, we collected such statements from a major service, LinkNYC [2], which discussed the collection of *location* and *browsing history*, and asked participants for their perspective on the statements. Our motivation for selecting these statements lies in the fact that location and browsing history are two key private data objects that are relevant

to city-wide WiFi services, as Eckhoff and Wagner also mention in their work on accessing free WiFi in smart cities [21]. Note that our goal was not to find ambiguity in privacy policies or to evaluate the readability of the privacy policies, rather we reported our finding about what reasons participants mentioned for not to read it even though they are interested in it.

In the first case, we provided two statements about determining the location as shown in Listing 1 and asked participants what they think about those statements.

```
a) We do not collect information about your precise
 location.
b) We know where we provide WiFi services, so when you
 use the services, we can determine your general location
 .
```

Listing 1: Statements about determining user's location.

If considered together, these statements may look contradictory at face value (i.e., does not collect vs. determines location); however, they indicate that LinkNYC collects general/coarse location via its access point's location, but not the user's precise location. About 64.32% ($users_{exp}$= 62, $users_{potn}$= 66) of our participants correctly identified that the statements have a different but not opposite/contradictory meaning. However, 20.10% ($users_{exp}$= 21, $users_{potn}$= 19) incorrectly interpreted the statements to be contradictory, while 15.58% ($users_{exp}$= 16, $users_{potn}$= 15) participants incorrectly interpreted these statements as having the same meaning. This finding demonstrates that most participants would be able to reason about such ambiguity in privacy policies, even if they currently do not read them due to the task being time-consuming.

Similarly, we provided two statements about information collection as shown in Listing 2, and asked participants what they thought about those statements.

```
a) We collect information when you use the Services,
 including information used to facilitate your use of the
  services, such as access to third-party websites and
 services, including URL requests, destination IP
 addresses, configuration details, or other information
 necessary to provide access to the Services.
b) We will not store your browsing history or track the
 websites you visit when you use your personal device to
 access the services.
```

Listing 2: Statements about information collection.

The above statements are contradictory because while the first statement clearly states that LinkNYC collects URL requests and destination IP addresses, the second states that it does not track the browsing history/websites the user visits. Although one may argue the fine subtleties of collection vs storage in the two statements, we believe that the notion of collection in the first includes storage unless the service explicitly states that it will discard this information after the user's session. About 52.26% ($users_{exp}$= 48, $users_{potn}$= 56) participants interpreted these statements as opposite/contradictory in meaning, which aligns with our (conservative) assessment given, while 41.71% ($users_{exp}$= 44, $users_{potn}$= 39) participants interpreted the statements as being different but not opposite/contradictory in meaning. Only 6.03% ($users_{exp}$= 7, $users_{potn}$= 5) participants incorrectly interpreted these statements as having the same meaning.

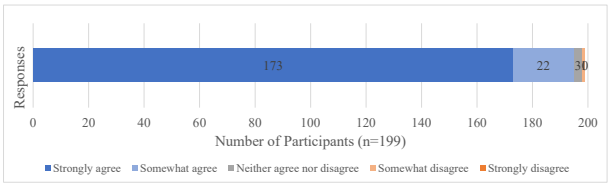

Figure 7: Participants' expectation to be informed about data collection

To summarize, while 64.32% participants were able to reason about statements in the first case, i.e., Listing 1 (with 82.81% or 106/128 having non-CS backgrounds), and 52.26% participants were able to reason about the statements in the second case, i.e., Listing 2 (with 83.65% or 87/104 having non-CS backgrounds). We find that about 33.67% (67/199) participants answered both questions correctly (with 88.06% or 59/67 having non-CS backgrounds).

Finding 12 ($\mathcal{F}_{12}$) – Several participants, i.e., over a third of the surveyed population, demonstrate the ability to correctly reason about complex information in privacy policies. However, they are nevertheless prevented from reading the policies due to their length and the time required.

This finding resonates with prior work, which has found readability to be the main barrier for not reading the privacy policies, and that users are not willing to spend time reading long or complex privacy policies [27].

4.4 Privacy Expectations

In Section 4.2, we discuss how users perceive privacy in the city-wide WiFi context. This section describes the findings from our analysis of participants' responses about what users expect from city-wide free WiFi services in terms of privacy, i.e., what services *should* do (**RQ3**). More specifically, we observe that participants (i) expect to be informed, (ii) expect to have rights and control over collected information and the process of collecting information, and (iii) expect to have a readable privacy policy, which we discuss in detail next.

Our participants overwhelmingly agree that they should be informed on how (and when) their data is collected and shared. When asked if they should be informed of data collection, 97.99% ($users_{exp}$= 97, $users_{potn}$= 98) participants agreed (including 86.93% strongly agreed) that they expect to know what personal information is being collected, as shown in Figure 7. Similarly, 95.98% ($users_{exp}$= 94, $users_{potn}$= 97) participants agreed (of which 82.91% strongly agreed) that they would like to get notified when asked whether they should be notified at the instance the data is collected. Moreover, we found that a significant number of participants expect the city-wide free WiFi services to *concretely* describe all the information about collection and names of the third parties the data would be shared with in their privacy policy. More specifically, 97.99% ($users_{exp}$= 96, $users_{potn}$= 99) participants agreed (of which 86.43% strongly agreed) that city-wide free WiFi services should mention all types of information they collect in their privacy policy and 92.46% ($users_{exp}$= 90, $users_{potn}$= 94) participants agreed (of

which 74.87% strongly agreed) that they would like to know about the names of third parties their data would be shared with.

Most of the participants expect to have significant control and rights over the information collected by WiFi services, and how it is collected. The participants know that since their information is collected by the WiFi service, the information could also be shared with other third parties. However, we found that participants expect to have the right to opt out of the sale/sharing of their personal data, primarily, as **P99** states, to *".. just to be sure that the information is safe"*. To elaborate, most participants agreed when asked whether they would like to have the right to opt out of the service sharing/selling their data, i.e., with 96.48% ($users_{exp}$= 95, $users_{potn}$= 97) agreeing (including 81.91% strongly agreeing). Similarly, 93.47% ($users_{exp}$= 91, $users_{potn}$= 95) participants (including 79.90% in strong agreement) agreed that they should have the right to delete their information.

Finding 13 ($\mathcal{F}_{13}$) – Participants expect city-wide free WiFi to inform them about privacy-sensitive data practices, such as how and why data is collected and shared, and expect to have rights and control over the collected data.

A similar sentiment is also observed among users in the context of smart buildings, i.e., Le et al.'s study with smart building occupants has shown that most of the occupants are concerned about their data being collected and want to be notified about the data collection [33].

As we discussed in Section 4.3, participants do not want to read privacy policy primarily because of long, verbose, legalese documents that require significant amount of time to read and understand its contents. Instead, participants expect a simple, short-/concise, and easily obtainable description of data privacy from city-wide free WiFi services that facilitates them by providing a quick review, resulting in seamless connection to the service while being cognizant of the privacy impact. As **P81** said,

> "*It should be written in a manner that is concise and easy to understand for all users. Important information should be up front and obvious.*"

Finding 14 ($\mathcal{F}_{14}$) – Participants expect a simple, short, and easily understandable privacy policy with all important information, to enable them to review the implications of using the service quickly, i.e., so that their access to WiFi is not delayed.

This expectation of a privacy summary is interesting, particularly given how participants are interested in reading privacy policies and can reason about complex/ambiguous statements, but at the same time, find policies long and verbose ($\mathcal{F}_{11}$), which deters them from actually reading them in practice. We discuss how these summaries, as our participants envision them, are similar to the work on privacy labels [29], but still different due to why users want them in this context, in Section 5.2.

5 Discussion

The findings of this study indicate that participants appreciate the utility of city-wide free WiFi ($\mathcal{F}_1$, $\mathcal{F}_2$), and believe that the services collect significant amount of private data ($\mathcal{F}_3$, $\mathcal{F}_4$). In fact, while participants are uncomfortable with the collection and sharing ($\mathcal{F}_5$, $\mathcal{F}_7$ – $\mathcal{F}_9$), most would trade off privacy for utility ($\mathcal{F}_6$, $\mathcal{F}_{10}$), just as prior work has observed in other contexts [16, 20]. However, some of the rationales for this trade-off are unique to the city-wide free WiFi context, i.e., participants place emphasis on the collector being a non-profit, governmental entity, and many would consent to the collection and sharing because they would *trust* the city to use the data for benign reasons, such as improving the service. We distill these and other key findings into three core themes that highlight noteworthy perceptions of and expectations from city-wide free WiFi services, and provide actionable takeaways for key stakeholders, including policymakers, researchers, and smart city WiFi providers.

5.1 The Privacy Paradox, and Trust

We observed that while more than half of the participants believe that city-wide free WiFi services collect personal information. In fact, participants are not comfortable with this collection, particularly given that the collector was a governmental, non-profit entity, who should have no use for selling the data, or using it for profit. Similarly, participants were uncomfortable with retention and sharing of their data, and indicated that they would not consent to the data being collected if they knew it would be shared with third parties. To summarize, participants were aware that city-wide free WiFi services indeed collect their data and were cognizant of the risks associated with the collection and sharing of it ($\mathcal{F}_5$,$\mathcal{F}_7$,$\mathcal{F}_8$,$\mathcal{F}_9$).

That said, we found that several participants, in spite of this awareness and concern for their privacy, would still trade it off for utility, which represents an instance of the *privacy paradox* [44] in this context. Particularly, participants indicated that city-wide free WiFi services were of significant value to them, despite usability issues, service disruptions, or privacy risks, and provided a desired alternative to cellular Internet due to their cost and availability ($\mathcal{F}_1$,$\mathcal{F}_2$,$\mathcal{F}_6$).

However, we believe that there is another factor that influences participants to trade-off privacy: the *trust* that they place in the non-profit nature of city-wide free WiFi services. To elaborate, participants expressed that they would be comfortable with this collection (and sharing) as long as it is for the improvement of the services, and to some extent trust city-wide free WiFi services to do so, given their non-profit nature, and the fact that they are operated by the government ($\mathcal{F}_{10}$). Participants similarly give services the benefit of the doubt in terms of the retention of this information, i.e., a majority believe that the services would not retain their data for the long term ($\mathcal{F}_7$). That is, unlike the privacy paradox uncovered in prior work, where utility is the only factor that prompts consumers to let go of their privacy, we find that this is indeed a unique instance of the paradox that is also influenced by the trust placed in the controller of information, which makes the privacy trade-off seem like a relatively *benign* choice.

5.2 Reforming Privacy Policies for City-wide WiFi Services

We observed that almost all of our participants have two expectations: to be informed about data collection and sharing practices, and to be notified at the time of collecting data. That is, users desire to be kept in the loop without impeding their access to the actual

service ($\mathcal{F}_{13}$). Surprisingly, most of the participants expressed that they tend to not read and would not be interested in reading the privacy policy specifically for city-wide free WiFi services, reasoning that privacy policies of other services tend to be long and difficult to comprehend because of legalese, and they assume it would be the same for city-wide free WiFi ($\mathcal{F}_{11}$).

How participants want to be in the privacy practices loop is a complex question that may yield several viewpoints. *One interpretation* of the results of this paper is that participants desire a short user-friendly privacy policy. That is, we observed that our participants expressed a need for summaries of privacy policies ($\mathcal{F}_{14}$), similar to the recent work on privacy labels [29] and policy summaries (e.g., Polisis [5, 26]). However, the motivation here is different: while prior work provides summaries to reduce the complexity inherent in privacy policies, several of our participants can reason about complexity ($\mathcal{F}_{12}$), but mainly seek to reduce the time spent reading a verbose policy, especially when connecting to WiFi, which is widely seen as a "plug-and-play" task.

To elaborate, participants favored quickly connecting to the WiFi, and did not want to spend too much time on reading privacy policy even if they could reason about the complex and ambiguous statements from the privacy policies. Instead, they shared that providing summaries of privacy policies that facilitates reviewing the privacy impact, while connecting to the WiFi network as quickly and seamlessly as possible would be desirable. That is, we find that privacy labels would be useful in the context of city-wide free WiFi services as well, and desired by users.

However, another way to interpret the results is that *social desirability bias* and a desire of being informed regarding the use of their data may have influenced the participants' viewpoints. To elaborate, it is also likely that our participants assumed that they would be inclined to read privacy policies if they were shorter/succinct; but there is no evidence at present to suggest that this desire to know about the privacy implications of city-wide free WiFi would translate into action in practice. In fact, as participants seek privacy disclosures without any delay in their access to the service ($\mathcal{F}_{13}$), it is entirely possible that this need for plug-and-play service may overcome their desire to read even summarized privacy disclosures.

To summarize, a key takeaway for service providers/cities is to provide a *privacy summary/label* on the sign-in page, which may encourage users to read the disclosures. However, we must also acknowledge that while this would be a good start toward making privacy disclosure effective in this domain, the user desire for summarized disclosure may not necessarily translate into adoption in practice.

5.3 Treating WiFi as a *utility* to Motivate Privacy Protections

As we discuss in Section 4.2, people are likely to sacrifice their privacy for their need to use city-wide WiFi services. Particularly, participants highlighted the inherent value in city-wide free WiFi services, especially in areas without cellular Internet ($\mathcal{F}_2$). That is, it may not be practical to treat city-wide free WiFi as a product/service that consumers can choose to use or avoid. Moreover, prior work found that consumers have a tendency to use free WiFi even if it is not secure [49]. Therefore, it may make more sense to treat city-wide free WiFi as a utility that most (if not all) people are likely to use it, and design privacy protections specifically for this particularly context.

To elaborate, while there are solutions such as privacy labels that focus on obtaining informed consent in the context of mobile/IoT product privacy, such solutions result in letting users decide whether they want to use or avoid the product, which is not applicable in the context of city-wide free WiFi. Our findings indicate that users may provide consent to data collection while still being uncomfortable with it, and sometimes, simply connecting to city-wide free WiFi may be considered as implicit consent to the privacy practices of the controller (e.g., as in the case of City of Boston's Wicked Free Wi-Fi [7]). Hence, a proactive approach that focuses on designing and adopting privacy-friendly policies and practices for public WiFi would be more effective, since consumers are going to consent anyway (despite being informed or knowing that their data would be collected and shared with third parties). Therefore, as a long-term solution, we argue that researchers, practitioners, and policymakers develop general criteria for acceptable privacy practices surrounding data extracted from users of city-wide WiFi deployments (which may contrast with privacy norms for for-profit/private ISPs, who do not have the same set of obligations to citizens).

A regulatory approach to this application domain might be feasible, drawing from the privacy regulations/norms/best practices that existing services provided by cities have to abide by. For instance, Washington State's RCW 19.29A.100 [3] regulates electric utility providers and prevents them from disclosing or selling any private consumer information (in contrast to city-wide WiFi services that are not directly regulated as such). Similarly, the Drivers Privacy Protection Act (DPPA) [1] protects personal information obtained by state Department of Motor Vehicles (DMVs), particularly regulating the circumstances under which they may use a driver's motor vehicle record. Finally, we note that general-purpose privacy legislations such as CPRA [6] do not apply to non-profit enterprises such as smart city WiFi services, further necessitating targeted legislation such as RCW 19.29A [3].

6 Limitations

While this work is the first to explore the privacy concerns among US users regarding city-wide free WiFi, the contributions of this paper should be examined in the light of the following limitations:

1. Validity of the findings within the US Context: As all of our participants are from the US, we acknowledge that the results of this study may be primarily valid within the US context, including both consumer perceptions/expectations, as well as legal implications of our findings. That said, given that the US has a growing number of cities that offer such city-wide Wifi services, this study offers impactful and actionable insights for key stakeholders in this locale. Further, we also emphasize that while this study is about the perceptions of "US users", it is entirely possible that US users may have traveled to non-US cities, and their responses may reflect their overall experiences. Moreover, our study design and methodology is sufficiently general, and can be adopted to understand the privacy perceptions of consumers in other locales with city-wide Wifi services, such as London, Dubai, Rome, Madrid, and South Korea.

2. Participant Recruitment and Balancing Demographics: We used Prolific to recruit participants for our study. While it is common to use crowdsourcing platforms like Prolific in user research, it is important to note that the participants from these platforms may not be representative of the average population [48]. As described in Section 3.3, we did not balance demographics during recruitment, given that the demographic distribution of the target population is unknown, and because our key goal during recruitment was obtaining a sufficient and balanced number of responses from experienced and potential users. Further studies are necessary in order to understand the demographic distribution of city-wide WiFi users in the wild, in order to determine what would constitute a representative sample.

3. Survey Design and Questions: The survey questions were influenced by prior literature [11, 21, 25, 27, 33, 38, 46] and the authors' experience in conducting such studies in data privacy, as well as feedback from our preparatory study. That is, we focused on common privacy considerations such as data collection, retention, sharing, and privacy policies of city-wide free WiFi. This design allowed us to provide a detailed overview of user perception about the privacy practices of city-wide free WiFi. However, we acknowledge that this approach may not capture all aspects of privacy concerns or practices, and that additional questions and resultant insights may be obtainable.

4. Bias, Self-reported Data: Similar to any survey-based study, our study may also be impacted by bias in self-reported data. That is, the participants reported their answers based on their recalled experience and perspectives, and hence, our findings may be affected by social desirability bias, as well as recall bias. As a result, while we checked the survey responses for completeness and quality, our study, like similar survey-based studies, cannot guarantee the veracity of the expressed experiences.

7 Conclusion

This paper explored perceptions and expectations of privacy practices among US users for city-wide free WiFi services. We found that most participants believe that city-wide free WiFi services collect personal information. However, they do not feel comfortable if the collected data is shared with third parties. Additionally, most participants wanted to be informed about the data collection practices, although they had yet to read the privacy policies of the city-wide WiFi services. This is because of their previous, ineffective interactions with privacy policies from other services, which were generally neither comprehensible nor concise. We also found that people tend to sacrifice their privacy for the need to use WiFi services, a behavior that may be influenced by the trust users place in city-wide free WiFi services. Given these findings, we provide recommendations for researchers, practitioners, and regulators, that may help in designing and adopting better, privacy-friendly city-wide free WiFi services in smart-cities. That is, city-wide free WiFi should be treated as a utility, and their privacy governed using regulations that are comparable to those governing utilities at present, aside from additional steps providers can follow to make the data practices easily understandable and transparent for users.

Acknowledgments

The authors would like to thank the revision editor, and the anonymous reviewers for their constructive feedback on the paper. The authors have been supported in part by the COVA CCI and NSF-2132281 grants. Any opinions, findings, and conclusions expressed herein are the authors' and do not reflect those of the sponsors.

References

[1] 1994. Drivers Privacy Protection Act (DPPA). https://epic.org/dppa/.
[2] 2015. LinkNYC. https://www.link.nyc.
[3] 2015. RCW 19.29A.100. https://app.leg.wa.gov/RCW/default.aspx?cite=19.29A.100.
[4] 2016. Pokemon GO. https://pokemongolive.com/.
[5] 2018. AI-powered Privacy Policies. https://pribot.org/.
[6] 2018. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa.
[7] 2023. CITY OF BOSTON WIRELESS WICKED FREE WI-FI PRIVACY POLICY. https://www.boston.gov/departments/innovation-and-technology/city-boston-wireless-wicked-free-wi-fi-privacy-policy.
[8] 2023. HOW WICKED FREE WI-FI WORKS. https://www.boston.gov/departments/innovation-and-technology/how-wicked-free-wi-fi-works.
[9] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L. Mazurek. 2021. Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 139–158.
[10] Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr Youssef. 2019. On privacy risks of public WiFi captive portals. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 80–98.
[11] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Tao Xie. 2019. PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play. In *Proceedings of the USENIX Security Symposium*.
[12] David G. Balash, Dongkun Kim, Darika Shaibekova, Rahel A. Fainchtein, Micah Sherr, and Adam J. Aviv. 2021. Examining the Examiners: Students' Privacy and Security Perceptions of Online Proctoring Services. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 633–652.
[13] David G. Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J. Aviv. 2022. Security and Privacy Perceptions of Third-Party Application Access for Google Accounts. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 3397–3414.
[14] Trevor Braun, Benjamin CM Fung, Farkhund Iqbal, and Babar Shah. 2018. Security and privacy challenges in smart cities. *Sustainable cities and society* 39 (2018), 499–507.
[15] V. Braun and V. Clarke. 2021. *Thematic Analysis: A Practical Guide*. SAGE Publications.
[16] Daniel J Butler, Justin Huang, Franziska Roesner, and Maya Cakmak. 2015. The privacy-utility tradeoff for remotely teleoperated robots. In *Proceedings of the tenth annual ACM/IEEE international conference on human-robot interaction*. 27–34.
[17] Ningning Cheng, Xinlei Oscar Wang, Wei Cheng, Prasant Mohapatra, and Aruna Seneviratne. 2013. Characterizing privacy leakage of public WiFi networks for users on travel. In *2013 Proceedings IEEE INFOCOM*. 2769–2777. https://doi.org/10.1109/INFCOM.2013.6567086
[18] Hoon S Choi, Darrell Carpenter, and Myung S Ko. 2021. Risk taking behaviors using public Wi-fi™. *Information Systems Frontiers* (2021), 1–18.
[19] Alberto De Marco and Giulio Mangano. 2021. Evolutionary trends in smart city initiatives. *Sustainable Futures* 3 (2021), 100052. https://doi.org/10.1016/j.sftr.2021.100052
[20] Roy Dong, Lillian J Ratliff, Alvaro A Cárdenas, Henrik Ohlsson, and S Shankar Sastry. 2018. Quantifying the Utility–Privacy Tradeoff in the Internet of Things. *ACM Transactions on Cyber-Physical Systems* 2, 2 (2018), 1–28.
[21] David Eckhoff and Isabel Wagner. 2018. Privacy in the Smart City Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 489–516. https://doi.org/10.1109/COMST.2017.2748998
[22] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.
[23] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2022. An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy* 20, 2, 31–39. https://doi.org/10.1109/MSEC.2021.3132398
[24] IS Farahat, AS Tolba, Mohamed Elhoseny, and Waleed Eladrosy. 2019. Data security and challenges in smart cities. In *Security in smart cities: models, applications, and challenges*. Springer, 117–142.

[25] Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376415

[26] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. 2018. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 531–548.

[27] Duha Ibdah, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. 2021. "Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies. *IEEE Access* 9 (2021), 166465–166487. https://doi.org/10.1109/ACCESS.2021.3130086

[28] Elvira Ismagilova, Laurie Hughes, Nripendra P Rana, and Yogesh K Dwivedi. 2022. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers* 24, 2 (2022), 393–414.

[29] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[30] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1573–1582. https://doi.org/10.1145/1753326.1753561

[31] Zaheer Khan, Zeeshan Pervez, and Abdul Ghafoor. 2014. Towards Cloud Based Smart Cities Data Security and Privacy Management. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*. 806–811. https://doi.org/10.1109/UCC.2014.131

[32] Ayca Kirimtat, Ondrej Krejcar, Attila Kertesz, and M. Fatih Tasgetiren. 2020. Future Trends and Current State of Smart City Concepts: A Survey. *IEEE Access* 8 (2020), 86448–86467. https://doi.org/10.1109/ACCESS.2020.2992441

[33] Tu Le, Alan Wang, Yaxing Yao, Yuanyuan Feng, Arsalan Heydarian, Norman Sadeh, and Yuan Tian. 2023. Exploring Smart Commercial Building Occupants' Perceptions and Notification Preferences of Internet of Things Data Collection in the United States. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE. https://doi.org/10.1109/eurosp57164.2023.00064

[34] Yibin Li, Wenyun Dai, Zhong Ming, and Meikang Qiu. 2016. Privacy Protection for Preventing Data Over-Collection in Smart City. *IEEE Trans. Comput.* 65, 5 (2016), 1339–1350. https://doi.org/10.1109/TC.2015.2470247

[35] Ahmed Y Lotfy, Alaa M Zaki, Tarek Abd-El-Hafeez, and Tarek M Mahmoud. 2021. Privacy Issues of Public Wi-Fi Networks. In *The International Conference on Artificial Intelligence and Computer Vision*. Springer, 656–665.

[36] David Maimon, Michael Becker, Sushant Patil, and Jonathan Katz. 2017. {Self-Protective} Behaviors Over Public {WiFi} Networks. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*. 69–76.

[37] David Maimon, C. Jordan Howell, Scott Jacques, and Robert C. Perkins. 2022. Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors. *Security Journal* 35, 1 (mar 2022), 154–174. https://doi.org/10.1057/s41284-020-00270-2

[38] Sunil Manandhar, Kaushal Kafle, Benjamin Andow, Kapil Singh, and Adwait Nadkarni. 2022. Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage. In *Proceedings of the 31st USENIX Security Symposium (USENIX)*. Boston, MA, USA.

[39] Antoni Martinez-Balleste, Pablo A. Perez-martinez, and Agusti Solanas. 2013. The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine* 51, 6 (2013), 136–141. https://doi.org/10.1109/MCOM.2013.6525606

[40] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[41] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[42] Jaron Mink, Amanda Rose Yuile, Uma Pal, Adam J Aviv, and Adam Bates. 2022. Users Can Deduce Sensitive Locations Protected by Privacy Zones on Fitness Tracking Apps *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 448, 21 pages. https://doi.org/10.1145/3491102.3502136

[43] Paolo Neirotti, Alberto De Marco, Anna Corinna Cagliano, Giulio Mangano, and Francesco Scorrano. 2014. Current trends in Smart City initiatives: Some stylised facts. *Cities* 38 (2014), 25–36. https://doi.org/10.1016/j.cities.2013.12.010

[44] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[45] Fayola Peters, Sorren Hanvey, Suresh Veluru, Alie El-din Mady, Menouer Boubekeur, and Bashar Nuseibeh. 2018. Generating Privacy Zones in Smart Cities. In *2018 IEEE International Smart Cities Conference (ISC2)*. 1–8. https://doi.org/10.1109/ISC2.2018.8656830

[46] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[47] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. "Warn Them" or "Just Block Them"?: Comparing Privacy Concerns of Older and Working Age Adults. *Proceedings on Privacy Enhancing Technologies (PoPETS)* (July 2021).

[48] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.

[49] Nissy Sombatruang, Lucky Onwuzurike, M Angela Sasse, and Michelle Baddeley. 2019. Factors influencing users to use unsecured wi-fi networks: evidence in the wild. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 203–213.

[50] Anna Ståhlbröst, Ali Padyab, Annika Sällström, and Danilo Hollosi. 2015. Design of smart city systems from a privacy perspective. *IADIS International Journal on WWW/Internet* 13, 1 (2015), 1–16.

[51] Statista. 2018. Number of public Wi-Fi hotspots worldwide from 2016 to 2022. https://www.statista.com/statistics/677108/global-public-wi-fi-hotspots/.

[52] Statista. 2020. Technology spending on smart city initiatives worldwide from 2018 to 2023. https://www.statista.com/statistics/884092/worldwide-spending-smart-city-initiatives/.

[53] VpnMentor. 2022. Research: Global Ranking of Free Wi-Fi Hotspots in 2022. https://www.vpnmentor.com/blog/free-wifi-hotspots-research/.

[54] Lingjing Yu, Bo Luo, Jun Ma, Zhaoyu Zhou, and Qingyun Liu. 2020. You Are What You Broadcast: Identification of Mobile and {IoT} Devices from (Public){WiFi}. In *29th USENIX Security Symposium (USENIX Security 20)*. 55–72.

[55] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen. 2017. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine* 55, 1 (2017), 122–129.

[56] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–20.

A Survey Instruments

Screening Survey

This is a screening survey to select eligible participants for a main study. In this survey, we will ask participants whether they have used city-wide free WiFi services. The screening survey is as follows:

. . . . . .

Consent Form *(We provide our consent form here)*
Do you consent to these terms?

- ○ Yes
- ○ No

(If 'No' is Selected: Since you have not consented to the survey, the survey will conclude here. Thank you.)

1 ***Some cities provide high-speed free WiFi services for the citizens so that the citizens can use them anywhere in the public places (e.g., New York's LinkNYC). Note: these free city-wide WiFi services do not include the WiFi services provided by the stores or restaurants. Have you ever used a city-wide free WiFi service?***

- ○ Yes
- ○ No

End of our screening survey

. . . . . .

Main Survey

Based on the responses from our screening survey, we invite participants who have used city-wide free WiFi services and who have not used those services yet. Participants who have used city-wide free WiFi services will answer one extra section 'User Experience' than the participants who have not used city-wide free WiFi services yet. Therefore, our main survey is as follows:

Consent Form *(We provide our consent form here)*
Do you consent to these terms?

- ○ Yes
- ○ No

(If 'No' is Selected: Since you have not consented to the survey, the survey will conclude here. Thank you.)

Section 1 of 6. *(This section is designed for participants who have experience with city-wide free WiFi services)*
In this section, we will ask questions about your experience of using city-wide free WiFi services. Questions will explicitly state if you can select multiple choices as answers.

1 ***Where have you used the city-wide free WiFi service? Please write the name of the city. (Please separate multiple city names with comma)***

2 ***How long have you used the service?***

3 ***What was your experience in using city-wide WiFi service?***

- ○ Extremely satisfied
- ○ Somewhat satisfied
- ○ Neither satisfied nor dissatisfied
- ○ Somewhat dissatisfied
- ○ Extremely dissatisfied

4 ***Please explain your response to the previous question.***

5 ***Have you ever read the privacy policy of the WiFi service you used?***

- ○ Yes
- ○ Maybe
- ○ No

6 ***Would you check your device's compatibility with the WiFi service before using the WiFi? (Example, some services may provide certain features only for compatible devices)***

- ○ Yes
- ○ Maybe
- ○ No

7 ***Please explain your response to the previous question.***

Section 2 of 6.
In this section, we will ask questions about your perspective on data collection of city-wide free WiFi services. Questions will explicitly state if you can select multiple choices as answers.

8 ***Do you think city-wide free WiFi services collect personal information from users?***

- ○ Yes
- ○ Maybe
- ○ No

9 ***What information do you think city-wide free WiFi services collect? Please select all that apply.***

- ☐ Name
- ☐ Email address
- ☐ Username
- ☐ Password
- ☐ Location
- ☐ Browsing history
- ☐ IP address
- ☐ Other (please specify) _____

10 ***How comfortable are you with the city collecting this information as a part of the WiFi service?***

- ○ Extremely comfortable
- ○ Somewhat comfortable
- ○ Neither comfortable nor uncomfortable
- ○ Somewhat uncomfortable
- ○ Extremely uncomfortable

11 ***Please explain your response to the previous question.***

12 ***What do you think of the following statement? "I have the right to know what personal information they collect"***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

13 ***How comfortable are you with city-wide free WiFi services requiring your email address to connect to the WiFi?***

- ○ Extremely comfortable
- ○ Somewhat comfortable
- ○ Neither comfortable nor uncomfortable
- ○ Somewhat uncomfortable
- ○ Extremely uncomfortable

14 ***How comfortable are you with city-wide free WiFi services determining your location when you use the service?***

- ○ Extremely comfortable
- ○ Somewhat comfortable
- ○ Neither comfortable nor uncomfortable
- ○ Somewhat uncomfortable
- ○ Extremely uncomfortable

15 ***What do you think of the following statement? "The city-wide free WiFi services should provide notification about data collection and purposes when using this service"***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

Section 3 of 6.
In this section, we will ask questions about your perspective on data storage/retention of city-wide free WiFi services. Questions will explicitly state if you can select multiple choices as answers.

16 ***How comfortable are you with the city-wide free WiFi services storing your information for later use?***

- ○ Extremely comfortable
- ○ Somewhat comfortable
- ○ Neither comfortable nor uncomfortable
- ○ Somewhat uncomfortable
- ○ Extremely uncomfortable

17 ***How long should they store the personal information?***

- ○ 1 month
- ○ 6 months
- ○ 1 year
- ○ 5 years or more / As long as they want
- ○ Not sure

18 ***What do you think of the following statement? "I should have right to request to delete my information"***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

Section 4 of 6.
In this section, we will ask questions about your perspective on information sharing of city-wide free WiFi services. Questions will explicitly state if you can select multiple choices as answers.

19 ***Do you think the city-wide free WiFi service may share your information with third parties?***

- ○ Definitely yes
- ○ Probably yes
- ○ Might or might not
- ○ Probably not
- ○ Definitely not

20 ***What information do you think city-wide free WiFi services share with third parties? Please select all that apply.***

- □ Name
- □ Email address
- □ Username
- □ Password
- □ Location
- □ Browsing history
- □ IP address
- □ Other (please specify) _____

21 ***What information do you think city-wide free WiFi services should be able to share with third parties? Please select all that apply.***

- □ Name
- □ Email address
- □ Username
- □ Password
- □ Location
- □ Browsing history
- □ IP address
- □ Other (please specify) _____

22 ***What types of entities do you think your information is shared with? Please select all that apply.***

- □ Service providers (i.e., entities through which the city provides WiFi)
- □ City's open data portal
- □ Advertisement company
- □ Companies with data sharing agreement
- □ Other (please specify) _____

23 ***If you know that the information collected by city-wide free WiFi services from you will be shared with third parties, would you still provide consent to such services to collect your information?***

- ○ Yes
- ○ Maybe
- ○ No

24 ***Please explain your response to the previous question.***

_____

25 ***What do you think of the following statement? "I should have right to opt out of sell/share of personal information"***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

Section 5 of 6.
In this section, we will ask questions related to privacy policy of city-wide free WiFi services. Privacy policy is a legal document where an organization states how they collect, store, use and share the information of the customers or users. Questions will explicitly state if you can select multiple choices as answers.

26 ***Would you be interested in reading the privacy policy of city-wide free WiFi services before using the service?***

- ○ Yes
- ○ Maybe
- ○ No

27 ***Please explain your response to the previous question.***

_____

28 ***Do you think city-wide free wifi services should mention all types of information they collect in their privacy policy?***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

29 ***Do you agree with the following statement? "City-wide free wifi service should mention the name of all the third parties they share the information with in their privacy policy."***

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

30 ***The following two statements have been collected from the same privacy policy of a city-wide free WiFi service. What do you think about these two statements?***
(i) We do not collect information about your precise location.

(ii) we know where we provide WiFi services, so when you use the services we can determine your general location.

- ○ These statements have the same meaning
- ○ These statements have the opposite/contradictory meaning
- ○ These statements have a different but not opposite/contradictory meaning

31 ***Please explain your response to the previous question.***

32 ***The following two statements have been collected from the same privacy policy of a city-wide free WiFi service. What do you think about these two statements about data collection? (i) We collect information when you use the Services, including information used to facilitate your use of the services, such as access to third-party websites and services, including URL requests, destination IP addresses, configuration details, or other information necessary to provide access to the Services. (ii) We will not store your browsing history or track the websites you visit when you use your personal device to access the services.***

- ○ These statements have the same meaning
- ○ These statements have the opposite/contradictory meaning
- ○ These statements have a different but not opposite/contradictory meaning

33 ***Please explain your response to the previous question.***

Section 6 of 6.

In this section, we will ask some questions about you.

34 ***How do you identify yourself?***

- ○ Male
- ○ Female
- ○ Non-binary
- ○ Prefer not to answer
- ○ Other _____

35 ***What is your age?***

- ○ 18-29 years old
- ○ 30-49 years old
- ○ 50-64 years old
- ○ 65 years or older
- ○ Prefer not to answer

36 ***What is your highest level of education?***

- ○ Less than high school
- ○ High school graduate
- ○ Some college
- ○ 2 year degree
- ○ 4 year degree
- ○ Masters
- ○ Professional degree
- ○ Doctorate
- ○ Prefer not to answer

37 ***Which of the following best describes your educational background or job field?***

- ○ I have an education in, or work in, the field of computer science, computer engineering, or IT
- ○ I do not have an education in, or work in, the field of computer science, computer engineering, or IT
- ○ Prefer not to answer

38 ***Which city do you currently live in?***

39 ***Is there anything else you would like to add related to this survey? (Optional)***

End of our main survey

Table 3: List of cities mentioned by participants. If a city name appears multiple times, we put the count (n) next to that city name.

List of cities			
Arlington	Asheville (2)	Atlanta (3)	Barcelona
Berlin	Boone	Boston (6)	Bountiful
Carrollton	Chicago	Cincinnati	Clemson
Copenhagen	Cumming	Dallas	Dover
Dubai	Dubuque	Durham	Edinburgh
Glasgow	Gowanda	Houston	Indianapolis (2)
Jacksonville	Kokomo	Las Vegas (2)	Liechtenstein
London	Los Angeles (3)	Louisville	Madrid
Manhattan	Meguro	Meridian	Merrillville
Miami	Minneapolis (3)	Mississippi	Monroe
Montesano	Nakano	Nashville	New Orleans
New York city (27)	Ocala	Omaha	Orlando
Osaka	Oxford	Paris	Philadelphia (3)
Pickerington	Redmond	Rio de Janerio	Riverside
Rome	Royalston	Sacramento	Salt Lake City
San Francisco (4)	Seoul	Shibuya	Shinjuku
Sioux falls (2)	Stockbridge	Stockholm	Tampa
Tokyo	Tulsa (2)	Vancouver	Walnut Creek
Washington DC	Wilkes-Barre	Yokohama	

B City Data Provided by Participants

Table 3 provides the list of cities mentioned by participants where they have used city-wide free WiFi:

We note that 14/99 (14.14%) of the participants mentioned more than one city in the referenced question. While this is a small percentage of the participants, we handled such cases in the following manner, from the survey design to the analysis stage.

First, the preamble of the section clearly stated that the participants would be asked about their "experience of using city-wide free WiFi services." That is, while we assumed experience with at least one service, the questions were always geared toward obtaining general experiences from using city-wide Wifi as a whole, regardless of one or more specific cities. Further, we followed up with an open-ended question requiring participants to provide additional context regarding their answer about their satisfaction with the service ("Please explain your response to the previous question"), in order for us to handle corner cases, if any. None of the 14 participants who mentioned multiple cities discussed city-specific attributes in response to this open-ended question; rather, one participant explained how city-wide WiFi in the multiple cities they traveled made it convenient to them as tourists. Others among these 14 provided non-city-specific responses (e.g., "some days are worse,

and some days are better..."), which also indicates that the participants answered the multiple-choice question regarding satisfaction with their overall experience of using city-wide WiFi services, without a specific city in mind. To summarize, the question regarding what cities the user had previously experienced WiFi services in was intended for data gathering, and not leveraged for analysis.