Online Privacy in Public Places: How do Location, Terms and Conditions and VPN Influence Disclosure?

Maria D. Molina
Media Effects Research Laboratory
The Pennsylvania State University
University Park, PA, 16802
mdm63@psu.edu

Andrew Gambino
Media Effects Research Laboratory
The Pennsylvania State University
University Park, PA, 16802
aug268@psu.edu

S. Shyam Sundar
Media Effects Research Laboratory
The Pennsylvania State University
University Park, PA, 16802
sss12@psu.edu

ABSTRACT

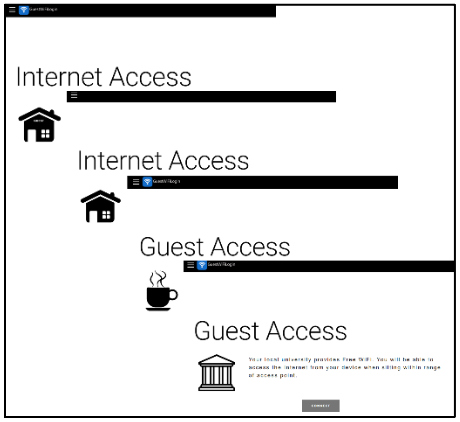
Do we disclose more information online when we access Wi-Fi from home compared to the University, or an Airbnb rental, or a coffee shop? Does it matter if we are shown terms and conditions (T&C) before getting online? Will signing into a virtual private network (VPN) affect our disclosure? We conducted an experiment (N = 276) to find out. Our results suggest that while VPN promotes disclosure of personal information and unethical behaviors in an Airbnb network, the provision of T&C inhibits this disclosure. Conversely, in a University network, provision of terms and conditions encourages disclosure of unethical behavior, but the presence of VPN cue inhibits it. Further, a user's belief in the publicness heuristic (public networks are risky) dictate how much users reveal in various locations based on their perceptions of relative security of accessing Wi-Fi from those locations.

CHI'19 Extended Abstracts, May 4–9, 2019, Glasgow, Scotland UK.

ACM ISBN 978-1-4503-5971-9/19/05.
https://doi.org/10.1145/3290607.3312932

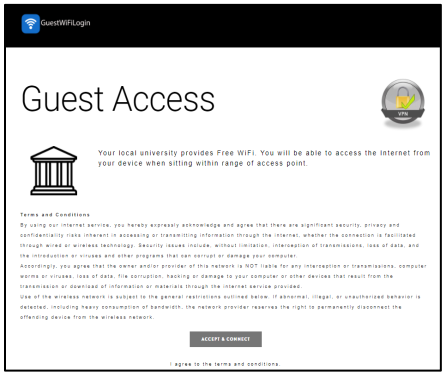
KEYWORDS

Privacy; Location; VPN; terms and conditions; Publicness Heuristic



Your local university provides Free WiFi. You will be able to access the Internet from your device when sitting within range of access point.

Figure 1: Stimulus indicating to participants the Wi-Fi network they were connecting to.



Guest Access

Your local university provides Free WiFi. You will be able to access the Internet from your device when sitting within range of access point.

Terms and Conditions

By using our internet service, you hereby expressly acknowledge and agree that there are significant security, privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology. Security issues include, without limitation, interception of transmissions, loss of data, and the introduction or viruses and other programs that can corrupt or damage your computer.

Accordingly, you agree that the owner and/or provider of this network is NOT liable for any interception or transmissions, computer worms or viruses, loss of data, file corruption, hacking or damage to your computer or other devices that result from the transmission or download of information or materials through the internet service provided.

Use of the wireless network is subject to the general restrictions outlined below. If abnormal, illegal, or unauthorized behavior is detected, including heavy consumption of bandwidth, the network provider reserves the right to permanently disconnect the offending device from the wireless network.

I agree to the terms and conditions.

Figure 2: Stimulus indicating VPN and terms-and-conditions statement location within the interaction.

1 INTRODUCTION

Mark Weiser's [12] dream of ubiquitous computing is becoming a reality, with students, workers, and travelers connecting to public Wi-Fi networks to accomplish their daily activities. It is not uncommon to find people using their laptops, tablets, and smartphones in coffee shops, airports, or universities. The Wi-Fi access available in many public places affords us the ability to get online nearly anywhere. A concern in these instances is that of security; are users mindful of security risks?

Despite the common belief that decision- making online is effortful, extant research argues that this is not always the case. When assessing the costs and benefits of interactions and making privacy-related decisions, users are influenced by many factors, including bounded rationality [1] or the limited mental resources to evaluate all possible consequences of our actions. Therefore, they often rely on simple mental models, triggered by cues on the interface, as decision-making strategies. For example, a study investigating user's perceptions of privacy policies, or terms and conditions, revealed that people do not read them because their sheer presence triggers a feeling of privacy [9,4]. Users probably have a rule of thumb which says that if a site provides a privacy policy, then it is looking out for their welfare. Such rules of thumb, formally called "cognitive heuristics," are employed because they obviate the need for effortful processing of information, yet they influence users' assessment of the content being presented [11]. Studies following this approach have identified specific privacy-related heuristics, triggered by interface cues, that influence information disclosure [5], focusing on the implications of cues within specific platforms. Less is known about users' disclosure when their physical location varies. In our research, we focused on cues that pertain to information disclosure when accessing Wi-Fi in different locations, ranging from public to private. In addition, we assess whether the provision of a terms and conditions statement (T&C) by the Wi-Fi provider, and the presence of a VPN symbol on the interface influence information disclosure.

1.1 Location and Publicness

Advances in networks have blurred the line between public and private internet use. For example, the use a public Wi-Fi to check bank accounts or shop online are activities that require disclosure of private information. An important heuristic that plays a role in users' decision-making in these instances is the publicness heuristic or the tendency to instinctively distrust wireless networks, especially in public places. To verify the claim that a particular location cue triggers the publicness heuristic, individual differences in the accessibility of this heuristic should predict differential disclosure in locations of various levels of publicness. Thus, we analyze the role of the publicness heuristic by comparing participants' level of self-disclosure when connecting to Wi-Fi at a coffee shop or university with their disclosure from more private locations, like an Airbnb rental, or home, as a function of their belief in that heuristic, and posit:

H1: (a) The higher the belief in publicness heuristic, the lesser the information disclosure via Wi-Fi in public, compared to private, locations. (b) This relationship will be mediated by perceived security of the network.

Table 1. List of Outcome variables and their reliability

Variables	*Sample Items*
Unethical behavior disclosure[6] (*M*= 3.5, *SD*=1.95, *α*= .98).	"Have you ever looked at pornographic material?"
Ethical behavior disclosure[3] (*M*= 4.3, *SD*=.90, *α*= .85).	"I would never think of letting someone else be punished for my wrongdoings,"
Financial information disclosure[8] (*M*= 4.3, *SD*=.94, *α*= .85).	Rate your level of comfort in sharing the following information with us: "my debt/loan," "my income"
Personal information disclosure[8] (*M*= 4.80, *SD*=1.35, *α*= .90).	Rate your level of comfort in sharing the following information: "my age," "my religion"

Table 2. Moderator, mediator, and control variables

Variables	*Sample Items*
Perceived security[7] (*M*= 3.40, *SD*=1.52, *α*= .92).	"Using this WiFi network is secure"
Publicness heuristic[9] (*M*= 5.62, *SD*=1.34, *α*= .74)	"It is not secure to manage personal business in public"
Power use [10] (*M*= 5.23, *SD*=.98, *α*= .88)	"Using any technological device comes easy to me"

1.2 VPN Symbol

Virtual private networks (VPNs) provide virtual tunnels that hide users' original IP address, allowing to surf the web anonymously. Because VPNs encrypt user's online activity, cybersecurity experts recommend their use especially in public Wi-Fi networks. A common tendency in public places is to create our own bubble where we feel safe. A VPN symbol in an interface can trigger the bubble heuristic ("that everything that transpires within the bubble is safe"). The general lack of knowledge among users about VPNs and paucity of research investigating their perceptions do not permit us to pose a hypothesis, so we pose the following research question:

RQ1: What is the relationship between location of network connectivity and VPN cues in the interface, and online information disclosure?

1.3 Terms and Conditions (T&C)

In an effort to present users with information necessary to make rational decisions about their use, interfaces tend to disclose their policy statement or T&C, often including details about the collection and sharing of user data, as well as a legal policy regarding data loss. However, in reality, users rarely read these policies because these statements cue the transparency heuristic or the rule of thumb that 'if a website posts its terms and conditions or privacy policy then it is credible and automatically safe' [9]. Research has shown mobile app users who perceive greater transparency about how their information would be used trusted the app more [2]. However, users are more attentive of such privacy indicators when buying privacy-sensitive products [4]. Thus, we posit:

H2: (a) When connected to a public Wi-Fi network, the presence of a T&C policy (versus no policy) will elicit more disclosure of information. (b) This relationship will decrease when disclosing sensitive information.

While the publicness heuristic, VPN symbol, and presence of T&C may act independently, they could also have a combined effect because they have the potential to trigger overlapping privacy concerns. To assess this possibility, we pose the following research question:

RQ2: What is the interaction effect of location, T&C, and VPN cues on an interface upon users' disclosure of private information?

2 METHOD

To test our propositions, we conducted a 4 (Location: coffee shop, university, Airbnb, and home) x 2 (T&C: present, absent) x 2 (VPN: present, absent) full-factorial between-subjects online experiment.

2.1 Participants

Participants were recruited using Amazon Mechanical Turk. Only participants who recalled the network they connected to correctly answered whether they saw the T&C and recalled their location were included in the final analyses (N = 276). The sample consisted of 43.1% male and 56.9% female, of ages between 18-72 (*M* = 36.7, *SD* = 10).

2.2 Procedure

After acknowledging consent, participants were asked to imagine they were accessing the Wi-Fi network of their randomly assigned condition and were provided with a link simulating the typical interaction where a pop-up appears to connect to a Wi-Fi network. After following the steps provided to connect to the network, and clicking "connect," a banner displayed, stating "you have successfully connected to your local [location] network." Following this, participants were redirected to the questionnaire and were asked to keep in mind they were connected to their Wi-Fi and through VPN (when in the VPN condition) while answering questions.

2.3 Stimuli/Cues

A series of website interactions were created for the purpose of this study. Participants were presented with a Wi-Fi login indicating the location of the network (See Figure 1). For VPN conditions, a lock symbol with letters VPN was displayed. For T&C conditions, a brief policy was present, and the "connect" button was changed to "accept and connect" (Figure 2).

2.4 Measures

3.3.1 Outcome variables. Information disclosure was assessed through four types of disclosure: unethical behavior, ethical behavior, financial information, and personal information (Table 1).

3.3.2 Mediator and Moderator. Perceived security and participant's belief in the publicness heuristic was measured using scales from previous literature found in Table 2.

3.*3.3 Controls.* Participant's power use (Table 2), gender, age, education, and ethnicity were entered as control variables.

3.3.4 Manipulation Check. To check if the location variable performed as expected, we ran a one-way ANOVA to compare the perceived publicness of each Wi-Fi network (Table 3).

3 RESULTS

To test H2, RQ1 and RQ2, a 4 (Location: coffee shop, university, Airbnb, and home) x 2 (T&C statement: present, not present) x 2 (VPN: present, not present) multivariate analysis of variance (MANOVA) was conducted to examine the effects of the three independent variables on the four types of information disclosure. This analysis revealed a significant three-way interaction between location, T&C, and VPN, Wilks' $\Lambda = .86$, $F(12, 582.36) = 2.75$, $p = .001$, partial $\eta^2 = .05$.

The univariate analysis for the three-way interaction was significant for ethical behavior, ($F(3, 223) = 2.89$, $p = .04$, partial $\eta^2 = .04$) and personal information ($F(3, 223) = 2.84$, $p = .04$, partial $\eta^2 = .04$), and near-significant for unethical behavior disclosure ($F(3, 223) = 2.53$, $p = .058$, partial $\eta^2 = .03$). Bonferroni post-hoc comparison reveals that the statistically significant differences are in the presence of a VPN cue with or without T&C, specifically in the Airbnb network for ethical behavior disclosure (Table 4), in the Airbnb and coffee shop network for personal information disclosure (Table 5), and in the University network for unethical behavior disclosure (Table 6).

In support of H1, data revealed an interaction effect such that when connected to the coffee shop (compared to the Airbnb and home networks), those with a higher belief in the heuristic tended to perceive lower security (Figure 3). A series of moderated mediation analyses revealed that the belief

Table 3. Perceived Publicness

Location	*Mean (SE)*
Coffee Shop	6.04 (.22)^a
University	5.70 (.22)^a
Airbnb	4.52 (.24)^b
Home	2.44 (.19)^c

Note: Conditions without a subscript in common differ at p < .05, using Least Significant Difference comparison.

Table 4. Disclosure of ethical behavior for Airbnb network.

	No T&C	*T&C*
VPN	(*M* = 4.72, *SE* = .25)	(*M* = 4.33, *SE*= .36)
No VPN	(*M* = 3.74, *SE* = .26)	(*M*= 4.69, *SE*= .22)

Table 5. Disclosure of personal information for Airbnb and coffee shop network.

	Airbnb network		*Coffee Shop*	
	No T&C	*T&C*	*No T&C*	*T&C*
VPN	(*M* = 5.52, *SE* = .38)	(*M* = 4.26, *SE* = .35)	(*M* = 5.41, *SE* = .33)	(*M* = 5.49, *SE* = .42
No VPN	(*M* = 4.30, *SE* = .40)	(*M* = 5.05, *SE* = .34)	(*M* = 4.26, *SE* = .35)	*M* = 4.92, *SE* = .31)

Table 6. Disclosure of unethical behavior for the University network.

	No T&C	*T&C*
VPN	(*M*= 3.47, *SE*= .52)	(*M* = 2.20, *SE* = .80)
No VPN	(*M*= 3.25, SE = .44)	(*M* = 4.53, *SE* = .51)

in the publicness heuristic moderated the relationship between location and perceived security such that when connected to the coffee shop (compared to Airbnb and home network), the higher the belief in the heuristic, the lower the perceived security of personal information. Similar moderated mediation patterns emerged for unethical and ethical behaviors, but only for the home network.

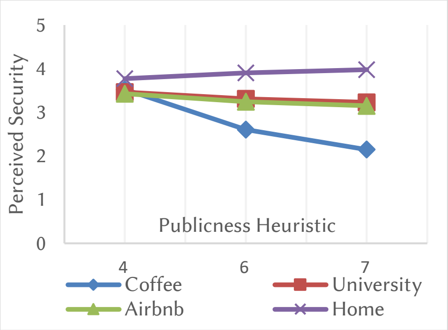


Figure 3. Interaction effect between location and publicness heuristic indicating the moderating role of publicness heuristic in the relationship between location and perceived security. *Note:* Significant differences were between coffee shop and Airbnb and coffee shop and home, *p*<.05.

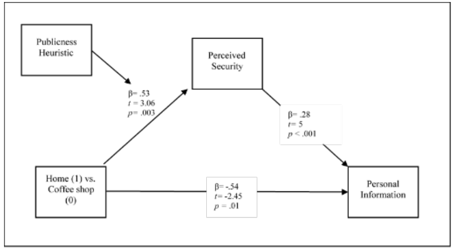


Figure 4. Moderated mediation analysis for personal information disclosure comparing home with coffee shop Wi-Fi, Moderated Mediation Index = .15 [CI: .034 - .285].

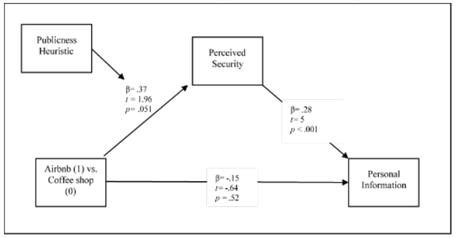


Figure 5. Moderated mediation analysis for personal information disclosure comparing Airbnb with coffee shop network, Moderated Mediation Index = .10 [CI: .002 - .223].

4 DISCUSSION

The three-way interaction between VPN, T&C, and location illustrates how privacy cues can backfire depending on the context of the connection. When disclosing information through the different network conditions, participants likely engaged in systematic or heuristic processing depending on their assessment of risk and uncertainty of the situation. When connecting to the University network, the presence of VPN might have given users a sense of security. serving its function of triggering the bubble heuristic and eliciting a feeling of safety from possible privacy threats. However, when both VPN and T&C were present, users perceived an increased risk, possibly because multiple cues alerted them about potential safety concerns of their information being accessible by multiple parties. It is also possible that users may have read the T&C statement as a disclosure from the network indicating that they will be giving away privacy in return for access; thus, they were less willing to disclose about their unethical behaviors. Another interpretation is that users thought the VPN was maintained by the University, alerting them to risky implications of disclosure.

In the Airbnb network, disclosure of personal information was higher when the VPN was present and the T&C was absent. One possibility is that the presence of the T&C cued participants to the downsides of VPN. Because users have the incorrect idea that T&C are an automatic sign of protection, it might be that users in the Airbnb location see the VPN as a “breach” of that protection, and thus feel safer disclosing without it. Conversely, it is also possible that in the presence of both cues, users interpret the VPN cue as a permission for VPN providers to log their information, increasing uncertainty about the security of information.

The moderating role of user’s belief in the publicness heuristic provides further support for the cue-heuristic solution to the privacy paradox [5]. Those who believed more in the publicness heuristic perceived a public network (coffee shop) as less secure than their home Wi-Fi, in turn disclosing less information. While these results are promising, they indicate a need to leverage these positive heuristics for ethical design practices. This is especially important given users were fairly consistent in the disclosure of their information in the coffee shop (despite being the most public space) where disclosure was fairly similar regardless of VPN or the presence of the T&C statement.

Similarly, despite being in an unknown network, participants rated the Airbnb network as less public than the university or coffee shop and were more willing to disclose when the T&C cue was present and without a secure VPN connection. It is possible that being in a digital space labeled “private” gives users a sense of security or that they viewed the T&C statement as a tradeoff between usage of the network and their privacy. However, as evidenced by our data, VPN impinged on this feeling of security by reducing personal information disclosure. Thus, it seems in some contexts the sheer presence of the VPN symbol alerts users to potential risks. It is important to keep in mind that these findings were based on an imagined scenario. The noted effects would likely be stronger in actual user interactions in the locations under study.

It is worth noting that more than half the participants did not even notice the VPN cue, which speaks to the limited mental resources allocated to process information related to privacy decision-making, or lack of knowledge about VPNs. Even though a T&C statement and VPN can alert users to security risks, they are contingent upon users realizing the presence of the cues on the interface.

The findings suggest opportunities for future design of cues signaling VPN and T&C (Table 7). While the lock symbol in the current design seems to reassure some users, it is not always seen as a protective bubble. Additionally, when co-present with T&C, the VPN cue seems to be interpreted as an alert suggesting that the Wi-Fi provider is in control of network traffic, inhibiting users' level of disclosure. Better design of cues and clearer communication of services are needed to combat misperceptions and better convey the value of protecting one's access to online networks in public.

Table 7. Design suggestions

Interface Cue and Heuristics	**Design Suggestion**
VPN	Instead of a lock or as complement, designers could: - Describe VPN allows to surf anonymously: "VPN: anonymous browsing" or "VPN: secure browsing" - Include a Wi-Fi symbol next to the lock signaling secure Wi-Fi. Clarifying what a VPN is could incentivize people to use this technology.
Publicness Heuristic	Cues that can trigger this heuristic include: - Warning signs: "Warning: this is a public network," "Warning: this is not your home network," "Warning: this is an unknown network." - Icons signaling the publicness of a location: "remember that you are in a coffee shop network" - Icons indicating risk of exposure to high traffic network or that the user is in roaming mode.

ACKNOWLEDGMENT

This research is supported by the U. S. National Science Foundation (NSF) via Standard Grant No. CNS-1450500.

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1: 26–33.

[2] Tsai-Wei Chen and S. Shyam Sundar. 2018. This app would like to use your current location to better serve you: Importance of user assent and system transparency in personalized mobile services. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18)*, ACM, New York, NY, USA, 254-268. DOI: https://doi/10.1145/3173574.3174111

[3] Douglas. P. Crowne and David Marlowe. 1960. A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology* 24, 4: 349–354.

[4] Serge Egelman, Janice Tsai, Lorrie Cranor, and Alessandro Acquisti. 2009. Timing is everything? The effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'09)*, ACM, New York, NY, USA, 319–328. DOI: https://doi/10.1145/1518701.1518752

[5] Andrew Gambino, Jinyoung Kim, S. Shyam Sundar, Jun Ge, and Mary Beth Rosson. 2016. User disbelief in privacy paradox: Heuristics that determine disclosure. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI' 16)*, ACM, New York, NY, USA, 2837–2843. DOI: https://doi/10.1145/2851581.2892413

[6] Leslie K. John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research* 37, 5 (February 2011), 858–873.

[7] Muniruddeen Lallmahamood. 2007. An examination of individual's perceived security and privacy of the internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce* 12, 3, 1-26.

[8] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs* 41, 1, 100–126.

[9] S. Shyam Sundar, Jinyong Kim, and Mary Beth Rosson. 2019. The role of interface cues in online privacy: Cognitive heuristics that predict information disclosure. In *69th Annual Conference of the International Communication Association (ICA)*, Washington, DC.

[10] S. Shyam Sundar and Sampada S. Marathe. 2010. Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research* 36, 3: 298–322. DOI: 10.1111/j.1468-2958.2010.01377.x

[11] S. Shyam Sundar. 2008. The MAIN model: A heuristic approach to understanding technology effects on credibility. *Digital media, youth, and credibility.* The MIT Press, Cambridge, MA, 72–100.

[12] Mark Weiser. 1993. Ubiquitous computing. *Computer* 26, 10: 71.