Understanding Privacy Attitudes and Concerns Towards Remote Communications During the COVID-19 Pandemic

Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, Franziska Roesner
Paul G. Allen School of Computer Science & Engineering
University of Washington

Abstract

Since December 2019, the COVID-19 pandemic has caused people around the world to exercise social distancing, which has led to an abrupt rise in the adoption of remote communications for working, socializing, and learning from home. As remote communications will outlast the pandemic, it is crucial to protect users' security and respect their privacy in this unprecedented setting, and that requires a thorough understanding of their behaviors, attitudes, and concerns toward various aspects of remote communications. To this end, we conducted an online study with 220 worldwide Prolific participants. We found that privacy and security are among the most frequently mentioned factors impacting participants' attitude and comfort level with conferencing tools and meeting locations. Open-ended responses revealed that most participants lacked autonomy when choosing conferencing tools or using microphone/webcam in their remote meetings, which in several cases contradicted their personal privacy and security preferences. Based on our findings, we distill several recommendations on how employers, educators, and tool developers can inform and empower users to make privacy-protective decisions when engaging in remote communications.

1 Introduction

The world was hit by a pandemic caused by the novel coronavirus and the COVID-19 disease in December 2019. In an attempt to prevent the spread of the virus, businesses and schools around the globe shut down, and people began sheltering in their homes to practice social or physical distancing [1].

Following social distancing protocols, people around the world have been encouraged or ordered to stay at home [2–4]. Hence, they started to work from home [5], keep in touch with family and friends remotely [6], and/or take remote courses [7], many for the first time [8]. This made remote conferencing tools an essential part of people's day-to-day lives, which albeit useful, posed potential privacy risks to people who are now regularly streaming video and audio from their own homes [9–15].

Increasingly integrated into people's lives and routines, widespread remote communications will not disappear with the end of the pandemic [16]. As people continue to work, socialize, and learn from home, it becomes imperative for their privacy and security to be protected. This requires the designers of in-home technologies (e.g., conferencing tools) and organizations that use them to understand the diverse needs of users. Understanding users' needs will enable designers and organizations to i) inform users about potential risks, and ii) gear their designs toward enabling users to control their privacy and security when using such technologies.

To that end, we conducted a worldwide survey ($n = 220$) on Prolific [17] in May 2020, i.e., a few months into the pandemic, as people were newly settling into widespread remote communications. We sought to conduct our study during the transition phase of the COVID-19 pandemic, when participants were still adjusting to their new remote settings, while remembering their normal lives before the pandemic. Our survey covered three contexts of remote communications, namely work from home (WFH), socialize from home (SFH), and learn from home (LFH). In each context, without priming participants by asking directly about privacy and security, we leveraged participants' open-ended responses to tease out their unbiased privacy and security attitudes and behaviors towards three aspects of remote communications: conferencing tools, modes of remote communications (microphone, webcam), and locations of remote communications. We conducted quantitative and qualitative analyses to answer the following three research questions:

1. How do people engage with different aspects of remote

communications in each context during the pandemic?

2. How do privacy and security factor into people's behaviors and attitudes towards aspects of remote communications in each context?

3. What approaches can be used to effectively inform and empower users' privacy and security decision making related to remote communications in each context?

We also designed our survey to allow us to explore related research questions for two other technologies that we hypothesized people would interact with more and/or have a new relationship with during the pandemic stay-at-home orders, namely smart home devices and social media platforms. Upon analyzing our results, we found that most participants' privacy and security concerns toward these two technologies did not change during the pandemic. Stay-at-home orders, however, significantly impacted participants' concerns and behaviors toward remote communications, which we primarily focus on in this paper. We include the survey questions on smart home devices and social media platforms and a summary of their findings in the extended version of our paper [18].

When being asked about conferencing tools, participants expressed a lack of decision-making agency. In WFH and LFH, participants reported to use the tool that was being decided for them by their employer or educator. Moreover, in all contexts, participants felt that they had no control over activating their webcam/microphone during their remote communications. For several participants, such imposed requirements contradicted their privacy and security preferences.

We found that participants' privacy attitudes and concerns towards the physical locations where their remote communications take place are context-dependent. By qualitatively analyzing participants' open-ended responses, we identified two types of location-related privacy: remote privacy (privacy from meeting attendees) and co-inhabitant privacy (privacy from household members). The open-ended responses suggested that in SFH, participants are mainly concerned about their co-inhabitant privacy, while valuing both remote and co-inhabitant privacy in WFH and LFH.

Based on the outcomes of our study, we distill several recommendations for organizations and tool developers on how to more effectively enable users to make informed and privacy-protective decisions with regard to their remote communications. In particular, we propose to enhance users' decision-making process by means of inclusive, transparent, and flexible policies on remote communications and designing privacy-protective features, which consider diverse and context-specific privacy and security needs.

2 Background and Related Work

Since December 2019, people around the world have been struggling with SARS-CoV-2 (novel coronavirus) and the resulting COVID-19 pandemic [19]. To help prevent further

spread of the virus, many people have exercised social or physical distancing, i.e., keeping a safe distance from others who are not from the same household [20]. Consequently, people started working, socializing, and learning from home. As a result, the use of conferencing tools and audio and video communications has increased dramatically.

2.1 Privacy and Security Risks of Conferencing Tools

The pandemic has redefined home from a place of *privacy and security* [21] to a shared work, socializing, and learning space. This sudden shift from in-person to remote interactions has led to an unprecedented increase in the use of remote communication tools [22]. Teleconferencing and video conferencing tools, such as Zoom [23], Microsoft Teams [24], Google Hangouts [25], and WebEx [26], have all seen a massive rise in usage thanks to people working, socializing, and learning from home.

As people started to increasingly rely on such tools for their daily communications, experts have become more concerned about the wide range of privacy and security risks these tools expose their users to [9–12]. A few of the reported concerns include Zoombombing [27], undisclosed data mining [28], and selling information to third parties [29]. By considering the context around remote communications, literature has discussed the privacy and security concerns involving remote health-related sessions [30, 31], educational communications [15, 32–34], attending online courses [35, 36], and work-related meetings [14, 37, 38].

Experts have provided several guidelines aiming to prevent the risks and mitigate the potential harms of conferencing tools [39–41]. Despite being valuable sources of information, these guidelines put the burden of protecting privacy and security mainly on the user. This is an unrealistic expectation due to several reasons. Confirming the literature [42], our findings showed that privacy and security aspects, although being important, are not always the number one priority when using and interacting with conferencing tools. Moreover, our qualitative findings suggested that due to their roles in their organizations, users often have limited power in making privacy-protective decisions, especially in work- and education-related contexts. In addition, the best practices reported in the current guidelines constitute a broad recipe, hoping that they apply to all users in all contexts of remote communications. From the literature, we already know that privacy is context-dependent [43].

2.2 Home Audio and Video Broadcasting

During the pandemic, people started to rely more and more on the microphones and webcams of their devices to stay in touch with their colleagues, friends and family members, or their classmates. Only a few weeks into the pandemic, the market saw a 179% jump in the sales of webcams [44], followed by

a supply shortage [45–47].

Privacy and security experts have indicated that webcams and microphones are susceptible to risks and vulnerabilities. Several reports showed how easily hackers take control of users' devices and activate their built-in webcam and microphone by exploiting the device vulnerabilities [48–53]. During the pandemic, in all contexts of remote communications, users are at an even higher risk of such hacking incidents as they are spending an increased amount of time using their webcams and microphones in different locations of their homes to remotely communicate with others [54]. Users might not be aware that their webcams and microphones are turned on as the LED indicator lights are not always effective [55] or they might have been deactivated by the attacker [56, 57].

To prevent hacking attacks from happening, experts frequently recommend users to cover their webcams and microphones when they are not being used [58, 59]. During the pandemic, however, users might not be able to diligently exercise this protective approach as many are encouraged or even forced to have their webcams and microphones on all the time. Employers are setting always-on webcam policies to encourage spontaneous chats among employees [60] and using surveillance tools to closely monitor the activities of their workforce [61, 62], in some cases even without users' knowledge [63]. Saying no to such surveillance is not always easy, especially during the pandemic with the heightened risk of unemployment due to potential retaliations [64].

Remote learning is not immune to such commonplace imposed surveillance as well. School-issued devices are not transparent about whether they spy on students by activating their webcams and microphones [65]. Some schools use proctoring software that enables access to the students' webcams and microphones during the exams [66, 67]. In addition, policies are in place forcing students to have daily audio and video interactions with their peers or teachers [68].

The aforementioned privacy-invasive webcam and microphone policies and surveillance practices allude to the ineffectiveness of the blanket and commonly referenced solutions with respect to the rising risks of these technologies. Designing privacy-protective tools and providing usable privacy and security guidelines for users require a deep understanding of users' decisions and behaviors. Our study contributes to the body of literature by providing novel empirical evidence, which highlights the significant impact of the context of remote communications, as well as the living conditions, on attitudes and privacy concerns related to remote communications.

3   Methods

We launched an online worldwide survey ($n =$220) on Prolific in May 2020. We initially recruited 230 participants and excluded 10 of them: 3 participants used the open-ended boxes to advertise a product and 7 participants provided other ir-

relevant responses to open-ended questions. We provide the complete list of survey questions in Appendix A, and we mention the question number in parenthesis (e.g., CQ1) when referring to each survey question in the remainder of this section. The study protocol was approved by our Institutional Review Board (IRB).

3.1   Participant Recruitment

We recruited prolific participants who were at least 18 years old. Because of the worldwide impact of the COVID-19 pandemic, we did not restrict our respondents to a specific region and instead, recruited participants from all around the world. The survey took on average 16 minutes to be completed, and we compensated each participant with US$5.

3.2   Survey Procedure

We started the survey by introducing our study to be about "technology use in the home during the Coronavirus (COVID-19) Pandemic." We then asked a few questions to obtain participants' consent to participate in our study (see Appendix A.1).

We asked questions on three contexts of remote communications: working from home (WFH), socializing from home (SFH), and learning from home (LFH). In the survey, we showed questions related to each context in a separate block. We randomized the order of these blocks to mitigate the potential order bias [69]. We asked similar questions in the three tested contexts and only changed how we referred to remote communications in each context. Specifically, in the contexts of WFH, SFH, and LFH, we referred to remote communications as "remote work-related meetings," "remote personal meetings with friends and family members," and "remote learning-related meetings," respectively.

3.2.1   Context-Specific Questions

To control for participants' familiarity with the contexts of remote communications, at the beginning of each context, we asked participants to specify whether they have experience with remote communications in that context (CQ1). We implemented a logic so that respondents could see the remaining questions of that context only if they reported to have experience with the context in question.

To better understand our participants' timeline for remote communications, we asked questions to capture when they started remote communications and how often they were engaged in remote communications before and during the pandemic (CQ2-4). In each context, we explored participants' attitudes, behaviors, and privacy concerns related to three aspects of remote communications: conferencing tools (CQ5-10), modes of remote communications (CQ11-14), and locations of remote communications (CQ15-19).

To understand what our participants were most concerned about in their remote communications, at the end of each context, we asked respondents to specify the incidents that happened to themselves or others that they perceived to be

concerning or awkward (CQ20-22).

3.2.2 Demographics and Home Settings

Finally, we asked questions to understand participants' demographic information, as well as their home settings (DH1-16). We placed the demographic questions at the end of the survey to minimize the possibility of stereotype threat [70–72].

3.3 Data Analysis

To analyze responses, we conducted qualitative and quantitative analyses.

3.3.1 Qualitative Analysis

The first author was the primary coder, who created the codebook for each open-ended question and kept it updated throughout the coding process. To analyze the data, we applied structural coding [73], which is a question-driven qualitative coding approach to categorize the interview data as well as open-ended survey responses [74]. The codebook consists of main and sub codes. The main codes are created from the topics of interest in the study. For example, we were interested in understanding what factors led participants to use specific conferencing tools during the pandemic. In the codebook, the main code we used to answer this research question was *reasons to use conferencing tools*, which was then divided into 11 sub-codes (e.g., *functionality*) and further divided into 8 sub-sub-codes (e.g., *convenience and accessibility*). After the codebook was created, the first two authors used the codebook to independently code all the open-ended responses. Authors had several meetings to go over the codebook and the coded responses and resolve the conflicts stemming from mismatched understandings of the codebook. After agreeing on the definitions used in the codebook, the first two authors re-coded all the responses. The final codebook consists of 11 main codes, 122 sub-codes, 54 sub-sub-codes, and 4 sub-sub-sub-codes. For each codebook, the Cohen's Kappa inter-coder agreement was calculated after the second round of coding. The average rate of agreement for all the codebooks was above 0.91, with a minimum of 0.88 and a maximum of 1. Based on the literature, Cohen's Kappa inter-coder agreement of over 0.75 is considered as "excellent" [75]. We provide the final codebooks in Appendix B.

3.3.2 Quantitative Analysis

We fit $M = 4$ Cumulative Link Mixed Models (CLMMs) with logit as the link function to our collected data in order to explain the dependent variables (DVs) we asked our participants about. In each model, the DV is a categorical variable that can take multiple *ordinal* values, each of which we refer to as a *response category*. For all models, we treated participants' demographic and home setting factors as control variables. We considered Akaike Information Criterion (AIC) as the goodness of fit for the models [76]. We only report on demographic factors that helped the model fit significantly better than the model without them. It is important to note that we

did not include the interaction terms in the final regression models as they did not improve the model fit. For the mth model, $m \in \{1, \ldots, M\}$, we denote the number of possible response categories by J_m, and we denote the corresponding number of *observations*, i.e., the number of participants that answered the question corresponding to that model, by N_m. For the nth observation, $n \in \{1, \ldots, N_m\}$, we let Y_m^n denote the observed response category. As per the CLMM definition, for the mth model, $m \in \{1, \ldots, M\}$, the probability that the nth observation, $n \in \{1, \ldots, N_m\}$, falls in the jth response category or below, $j \in \{1, \ldots, J_m - 1\}$, is modeled as

$$\text{logit}(\Pr(Y_m^n \leq j)) = \alpha_{j|j+1} - u_{\texttt{participant}_n} - \sum_{i=1}^{I_m} \beta_{\texttt{IV}_{m,i}}^n,$$

where $\alpha_{j|j+1}$ denotes the threshold parameter or cut-point between response categories j and $j+1$, and $u_{\texttt{participant}_n} \overset{i.i.d.}{\sim} \mathcal{N}(0, \sigma_u^2)$ denotes the random effect for the participant in the nth observation. Moreover, $\{\beta_{\texttt{IV}_{m,i}}^n\}_{i=1}^{I_m}$ represent model coefficients corresponding to the I_m different independent variables (IVs) in the mth model, each particular to the level that was reported in the nth observation.

4 Results

We start this section by providing information on participants' demographics and timelines of remote communications. We then present findings on participants' behaviors and decisions related to three aspects of remote communications: conferencing tools, modes of remote communications, and locations of remote communications.

4.1 Participants

We recruited 230 participants (reduced to 220 after excluding invalid responses) on Prolific. Our participants were mainly from UK (31%), Poland (15%), and US (14%). 43% of our respondents were female and 57% were male. Most participants did not have a background in Information Technology fields (65%) and were 18-29 years old (62%). We provide details on participants' demographics, home settings, and timelines of remote communications in Appendix C. Except for questions on the consent form (see Appendix A.1), none of the survey questions required participants to provide an answer. For each finding, we specify the number of participants that answered the corresponding question.

4.1.1 Frequency of Remote Communications

When asked about the frequency of remote communications before the pandemic, responses suggested that participants had more experience with remote communications in the socializing context than work and learning contexts. During the pandemic, in the contexts of WFH and SFH, most participants (WFH: 150/220, SFH: 208/220) reported that they have been mostly having remote meetings and communications. In the
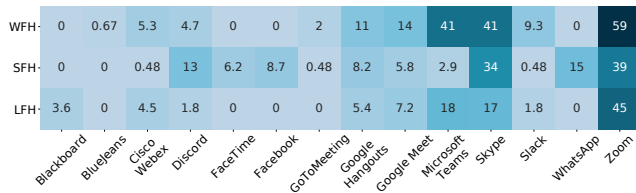
Figure 1: Usage of conferencing tools (in percentage) in different remote communication contexts reported by participants.

Figure 2: Participants' reported level of comfort with frequently used conferencing tools.

context of LFH, about half of our respondents (LFH: 114/220) reported to be having remote learning-related meetings.

Designing usable and privacy- and security-protective conferencing tools and guidelines in remote communications requires a deep understanding of users' attitudes and concerns towards remote communications. To this end, in our survey, we captured participants' context-specific thought process and decision making toward three aspects of remote communications during the pandemic: conferencing tools, modes of remote communications (webcam/microphone), and locations of remote communications. Without priming participants, we surfaced the role of privacy and security in participants' decision making related to each aspect of remote communications.

4.2 Conferencing Tools

In all contexts, Zoom was reported to be used more frequently than other tools (WFH: 35%, SFH: 27%, and LFH: 42%). We found that most participants (59%) were using the same conferencing tool for their WFH and LFH meetings and 35% of participants were using the same application in all three contexts. Figure 1 shows the fraction of participants who reported using each of the conferencing tools at least once for their remote communications across the three contexts.

In each context, on a five-point Likert scale, we asked participants to specify their level of comfort with the conferencing tool they most frequently use for their remote communications. Across all contexts, most participants (WFH: 87/150, SFH: 161/208, LFH: 75/114) were somewhat or very comfortable when using the conferencing tools for remote communications (see Figure 2). Our regression analysis indicated that the context of remote communications significantly impacts participants' level of comfort (see Table 1). We found that compared to work from home, participants were significantly more comfortable when using tools to communicate with family and friends (estimate = 1.43, p-value < 0.05) as well as communicating in the context of learning (estimate = 0.88, p-value < 0.05). Participants who reported to be using Google Hangouts were significantly more comfortable (estimate = 2.13, p-value < 0.05) with their conferencing tool than those who were using Zoom.

In each context, we explored participants' reasons behind their choice of conferencing tools as well as their comfort and discomfort wi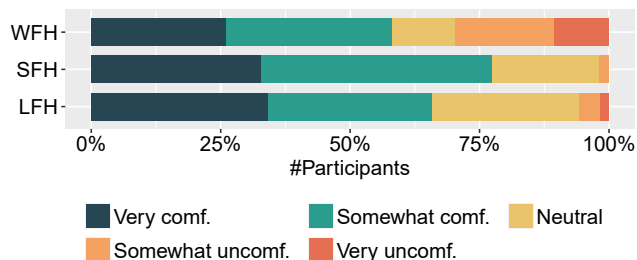th the tools. By qualitatively coding their open-ended responses, we surfaced several factors impacting participants' decision making and comfort level toward the use of conferencing tools.

4.2.1 Lack of Autonomy in Decision Making
In the contexts of WFH and LFH, participants frequently (WFH: 70/146, LFH: 64/107) implied that they have no agency over choosing what conferencing tool to use for their meetings. This lack of control was due to the fact that the tool was being selected for participants by their employers or educators, sometimes despite their personal preferences.

In the WFH context, some participants (WFH: 21/70) reported that the required conferencing tool is aligned with privacy and security preferences and requirements of their employers. P16 reported to be using Microsoft Teams for their WFH meetings: "Work requires me to only use this tool. They say this is the most secure one out there." Similarly P177 discussed why their employer asked them to use Microsoft Teams for WFH meetings: "It is the only tool that the company has approved security wise on our network."

In LFH, such imposed decisions contradicted some participants' (LFH: 17/64) personal privacy and security preferences, especially when they were required to use Zoom for their learning-related meetings. P36, who reported to use Zoom for their remote learning-related meetings, said: "That is the tool our teacher has chosen for us. Although security is certainly a problem."

4.2.2 Usability and Features
In all three contexts, the provided features and the usability of the tool were the second most frequently mentioned reasons to use the tool (WFH: 41/146, SFH: 92/204, LFH: 21/107) and the most commonly reported factors to make participants comfortable when using the conferencing tool (WFH: 75/111, SFH: 84/154, LFH: 42/70). P9, who frequently uses Microsoft Teams for their work meetings, said: "I can clearly see every file that's been attached to our meetings, I can easily contact with others and the quality of voice and video is just perfect." Unlike SFH, one of the most desirable features in the contexts of WFH and LFH was the ability of the tool to function properly with large groups. P102, who was using Zoom for their work meetings, said: "It supports a bigger number of people

Model No. and AIC	Dependent Variable	Independent Variable	Levels	Estimate	Odds Ratio	Std. Err.	*p*-value
1 (AIC=271.58)	Tool comfort level	Context (baseline=WFH)	SFH	1.43	4.18	0.56	*
			LFH	0.88	2.41	0.44	*
		Tool (baseline=Zoom)	Google Hangouts	2.13	8.41	0.81	*
			Google Meet	1.79	5.99	0.76	0.30
			Microsoft Teams	0.98	2.66	0.76	0.20
			Skype	0.80	2.23	0.74	0.27
		#Adults	$\{1,2,\dots\}$	−1.03	0.36	0.52	*
2 (AIC=266.71)	Microphone usage	Context (baseline=WFH)	SFH	1.53	4.61	0.39	***
			LFH	−1.61	0.20	0.33	***
		#Children (7-13)	$\{0,1,2,\dots\}$	1.29	3.63	0.44	**
3 (AIC=322.47)	Webcam usage	Context (baseline=WFH)	SFH	1.66	5.26	0.34	***
			LFH	−1.49	0.22	0.34	***
		Age (baseline=18-29)	30-49	0.98	2.66	0.46	*
			50-64	2.71	15.03	2.05	0.19
		#Rooms	$\{0,1,2,\dots\}$	0.31	1.36	0.14	*
4 (AIC=349.44)	Location comfort level	Context (baseline=WFH)	SFH	1.62	5.05	0.42	***
			LFH	0.66	1.93	0.36	0.06
		Location (baseline=Bedroom)	Dining room	−0.59	0.55	0.46	0.44
			Kitchen	−0.63	0.53	0.39	0.52
			Living room	−1.10	0.33	0.45	*
			Work room	−0.38	0.68	0.54	0.56
		#Adults	$\{1,2,\dots\}$	−0.56	0.57	0.28	*
		Gender (baseline=Female)	Male	1.04	2.83	0.42	*

Note: $*p < 0.05$ $**p < 0.01$ $***p < 0.001$

Table 1: Regression results of the CLMMs we built to explain participants' attitudes and concerns toward various remote communication aspects. A positive estimate of a level of an independent variable implies inclination toward an increase in the dependent variable and vice versa.

to be in a call better than the other ones."

In the WFH and LFH contexts, almost all participants (WFH: 40/41, LFH: 19/21) who mentioned using a conferencing tool based on its convenience and usability, reported to personally benefit the most from these attributes in their remote communications. P194 reported to be using Microsoft Teams for their WFH meetings: "Microsoft Teams allows me to stay connected more easily."

Unlike WFH and LFH, in SFH, several participants reported to use a conferencing tool mainly due to its perceived ease of use and convenience for others on the call (e.g., family members or friends), especially those with limited familiarity with technology. P90, who was most frequently using Skype to communicate with family members, said: "Parents are not confident with tech, Skype was the easiest for them to set up."

Some participants (WFH: 11/146, SFH: 9/204, LFH: 14/107) discussed giving up their privacy and security due to the tools' provided features and convenience. Almost all participants who mentioned such trade-offs reported to be using Zoom for their remote communications. In the context of WFH, P176 said: "Zoom offers the best features and is easy to use. Although security is certainly a problem." Users' trade-off between privacy and security and provided convenience is a known behavior in the literature [42, 77, 78].

4.2.3 Familiarity with the Tool

The most mentioned reason in deciding what conferencing tool to use to communicate with friends and family members was how familiar the tool was to participants themselves and also others on the call (SFH: 94/204). P54 reported to use WhatsApp for their SFH meetings to accommodate their family members: "It's the one my family have already installed on their phones and know how to use." Familiarity with the tool was the third most frequently mentioned reason in the contexts of WFH and LFH (WFH: 29/146, LFH: 15/107). P84 reported to use Skype more frequently than other tools: "The people I am calling with use Skype more than anything. I would rather use Zoom instead." Familiarity was also the second most commonly mentioned contributor to participants' comfort with conferencing tools (WFH: 22/111, SFH: 48/154, LFH: 15/70). P12 reported why they are comfortable with using Skype for their SFH meetings: "I have been using Skype since I was a teenager, so I'm used to it and that makes me more comfortable when I'm talking to friends and family."

Unlike WFH and LFH, in SFH 33% of participants, who reported to value the familiarity with the tool the most, implied that such familiarity partially stemmed from using the tool in contexts other than socializing (e.g., work, learning). P10 reported to use Microsoft Teams for their SFH meetings: "My

school uses the same platform and it's easier to be on only one platform at the same time."

Participants' open-ended responses implied how familiarity with the tool impacted their privacy and security concerns. A few participants (WFH: 9/29, SFH: 17/94, LFH: 6/15) perceived a sense of safety when using the tool due to their prolonged experience with the tool. P30, who used Discord for their personal meetings, said: "I know it is very safe and reliable because I've been using it for the past 3 years." This finding confirms the role of familiarity with technology in reducing risk perception [79]. Besides, a few participants associated their privacy concerns with their familiarity with the tool. P70 discussed why they only use Discord for their SFH meetings: "I already had account on it and also I am not comfortable sharing my info with more companies."

4.2.4 Privacy and Security Factors

In all three contexts, the perceived privacy and security of the tool were the third most commonly mentioned factors in making participants comfortable when using the tool for their remote meetings (WFH: 22/111, SFH: 20/154, LFH: 11/70). In WFH, Microsoft Teams and in SFH and LFH, Zoom were most frequently praised for their privacy and security practices.

When discussing their comfort with conferencing tools, some participants did not mention a specific privacy or security practice that made them comfortable when using the tool and instead said: "It is secure," "It feels like a safe app," or "I have no privacy concerns." We qualitatively coded the open-ended responses and identified several privacy and security best practices and perceptions that were frequently reported across all contexts:

- *Information being encrypted (7)*: WhatsApp:3, Zoom:4
- *Trusted brand (6)*: Microsoft Teams:2, Google Meet:1, Zoom:2, Cisco:1
- *No reported risk on media (6)*: Microsoft Teams:3, Cisco:1, WhatsApp:1, Discord:1
- *Protection from unauthorized access (5)*: Microsoft Teams:2, Google Meet:2, WhatsApp:1
- *Ability to set password for meetings (2)*: Zoom:2
- *No information being stored (1)*: Google Meet:1

Although most participants were comfortable with using the tools for their remote communications, some participants reported being somewhat or very uncomfortable (WFH: 17/150, SFH: 16/208, LFH: 7/114). Privacy and security were frequently mentioned as the reasons for participants' discomfort when using the tools (WFH: 8/17, SFH: 5/16, LFH: 3/7). Below is the list of privacy and security practices and beliefs that made participants uncomfortable when using the conferencing tool:

- *Risks and vulnerabilities reported by the media (7):* Zoom:7

- *Personal space being exposed in the meeting (4):* Zoom:3, Google Meet:1
- *Data being sold to third parties (2):* Zoom:2
- *Amount of information being collected (2):* Google Duo:1, Skype:1

We asked participants to specify how they manage their reported discomfort with the conferencing tools. In WFH and LFH, participants reported to address their concerns and discomfort by sharing less with other meeting attendees (WFH: 6/17, LFH: 2/7). Limiting the exposure was both in terms of restricting the content that is being shared, as well as modifying the configuration of their tool or the camera on their computer to limit the exposure. P4 limited the content they shared in the meeting and said: "I try not to say anything that could be used badly."

Unlike WFH and LFH, The most commonly mentioned mitigation approach in SFH was limiting or avoiding the use of the tool (SFH: 9/16). P188, who reported using Google Hangouts, said: "I will uninstall it as soon as it is no longer needed."

Some participants reported to take no action when being uncomfortable when using the tools (WFH: 4/17, SFH: 5/16, LFH: 1/7), mainly due to not being in charge of selecting the tools, not knowing what privacy and security controls the tool offers, or believing they have nothing to hide. P50 discussed why they do not take any action to address their privacy concerns with Google Duo: "Lots of other people use it too, nothing likely concerning will happen about what information the app ... collected on me."

4.3 Modes of Remote Communications

In all contexts, participants reported to activate their microphones significantly more frequently (p-value < 0.001) than their webcams when having remote communications (see Figures 3 and 4). Our CLMM results showed that compared to WFH, participants turned on their webcams (estimate $= 1.66$, p-value < 0.001) and microphones (estimate $= 1.53$, p-value < 0.001) significantly more often when having remote personal meetings with friends and family members, and significantly less often (webcam usage: estimate $= -1.49$, p-value < 0.001; microphone usage: estimate $= -1.61$, p-value < 0.001) when having remote learning-related meetings (see Table 1).

4.3.1 Microphone/Webcam Misuse

Accidental exposures of audio and video can lead to privacy violations. When asking participants about awkward incidents that had happened to them or others, across all contexts, the misuse of microphone and webcam was mentioned in almost all reported incidents (WFH: 29/34, SFH: 17/18, LFH: 8/10). In these incidents, the microphone and/or webcam were capturing unintended footage of a meeting attendee without their awareness and in some cases, without the awareness of the
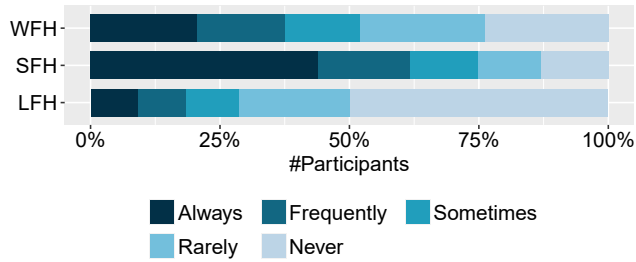
Figure 3: Reported frequency of using webcam.

Figure 4: Reported frequency of using microphone.

household members. For example, in WFH, P194 mentioned an incident involving the microphone: "A member of management did not remember to mute himself while he answered his personal phone on speaker with what sounded to be a lawyer." P185 reported a similar incident in LFH that involved the misuse of webcam in the meeting: "Someone in a classroom stood up naked on the Zoom call and I guess he didn't know until it was too late."

In order to raise users' risk awareness and prevent such incidents from happening, we need to understand the underlying reasons for participants' preferences towards different modes of remote communications. We asked participants how they decide to turn on their webcam and microphone when having remote communications.

4.3.2 Agency over Decision Making

Participants' reasons to activate their microphone/webcam in WFH and LFH meetings implied their lack of agency over sharing their audio/video in their remote communications. In these contexts, respondents reported that they were explicitly expected to activate their microphone/webcam as a direct request by their employer or educator (WFH-Webcam: 73/101, LFH-Webcam: 66/94, WFH-Microphone: 77/127, LFH-Microphone: 59/97). Psychology literature refers to this type of behavior as *obedience*, i.e., a form of social influence where group members change their behaviors and attitudes due to a direct request or command from an authority figure [80]. P101, who reported to always turn on the webcam in their remote work-related meetings, said: "There isn't a choice in terms of my manager requesting a meeting face to face." For some participants, such imposed requests contradicted their personal preferences. P75 discussed their lack of desire to activate their webcam in work-related meetings: "If the manager asks me to turn on the video, I have to do it, but I personally prefer to maintain it switched off at all times."

In LFH, several participants reported being required to have their webcam and microphone on when taking exams (LFH-Webcam: 19/66, LFH-Microphone: 23/97). P43 discussed how they decide on when to activate their webcam during learning-related communications: "It depends if I'm explicitly asked by the professor to turn it on (For example when I have an 'oral exam' since written exams are now hard to do remotely)."
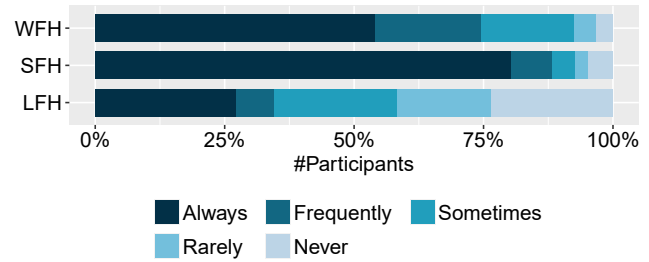
Although no participant reported to be explicitly requested by others to activate their microphone/webcam in SFH meetings, our qualitative analysis found the implicit expectation to be the main factor in participants' microphone/webcam usage. Most participants perceived lack of control over the use of microphone/webcam and reported that they are naturally expected to turn on their microphone/webcam when talking to their family and friends (SFH-Webcam: 134/208, SFH-Microphone: 166/208). P183 reported: "I always turn the webcam on during personal meetings with friends and family because I think it is what they expect and it would be rude not to."

Across all contexts, participants frequently mentioned that they would make the decision to activate their microphone/webcam based on other meeting attendees' behaviors (WFH-Webcam: 58/150, SFH-Webcam: 22/208, LFH-Webcam: 27/114, WFH-Microphone: 43/150, SFH-Microphone: 18/208, LFH-Microphone: 26/114). In LFH, P185 reported to sometimes turn on their webcam: "If other students have their cameras on I am more likely to turn mine on. But if nobody has theirs on, I will probably not turn on my camera." This type of social influence is called *informational conformity* [81], which serves as a cognitive repair [82] and happens when group members follow others' behaviors and directions as they are unsure about the appropriate behavior [83]. In several cases, participants reported to comply with the crowd despite holding a different preference. P43 reported to rarely turn on their webcam in work-related meetings: "Depending on the other person/people, and they always prefer to have a video. I personally find it a bit stressful, but don't mind it too much."

In SFH, some participants (SFH: 27/208) reported to jointly decide on the expectations around the use of microphone and webcam mostly prior to their personal meetings. P134 reported: "When we decide to meet, we choose video or none in the meeting invite." A few participants discussed the importance of joint decision making in accommodating meeting attendees' preferences. P160 reported to frequently turn on their webcam when meeting their friends: "If I miss seeing her face, we will plan a video call. We plan them because she has anxiety which I definitely want to accommodate for as

best [as I] can."

4.3.3 Attitudes over the Modes of Communication

Our participants shared diverse sentiments over activating their webcam/microphone in remote communications. In SFH, no participant suggested being uncomfortable with their lack of autonomy over webcam/microphone in their personal meetings. P117 discussed why they feel comfortable to always have their webcam on when meeting family and friends: "My family expect me to have video on, but I don't mind as I feel comfortable with people who really know me and accept me for who I am. I guess it's a gut feeling, if I don't feel anxious in their company in real life face to face, I would feel comfortable on a screen."

Unlike SFH, several participants (WFH: 21/101, LFH: 13/94) in WFH and LFH expressed negative attitudes toward having their webcam on. P80, who reported to activate their webcam at their employer's request, said: "I don't think video is necessary for the outcome of the meeting. It would be odd seeing colleagues in their home environment." P84 discussed why they do not feel comfortable with having webcam on in their LFH meetings: "I do not want to be seen by people I have never met, so I do not turn it on, unless I am being asked by the teacher." On the contrary, some participants (WFH: 16/101, LFH: 8/94) shared positive sentiments and supported having the webcam on during WFH and LFH meetings. P151, who reported to always turn on their webcam in WFH meetings, said: "I always turn it on as I feel face to face conversations with people create a better environment, and a higher level of honesty. I have campaigned for a policy in work to make video compulsory, and it has been taken up." P43 discussed why they preferred to have their webcam on in LFH meetings: "It is 'nice' and more productive during the Q&A meetings to have webcam on and discuss about issues/doubts about a particular project."

4.4 Locations of Remote Communications

We asked participants to specify which part(s) of their homes they most frequently use for their remote meetings. Across the three contexts, participants' bedroom (WFH: 56/150, SFH: 83/208, LFH: 49/114), living room (WFH: 32/150, SFH: 75/208, LFH: 25/114), and study or workroom (WFH: 38/150, SFH: 19/208, LFH: 21/114) were reported to be used more often than other locations. Despite being rare, a few participants reported using their bathrooms for their remote meetings (WFH: 3/150, SFH: 10/208, LFH: 1/114). Figure 5 shows the fraction of participants that reported to use each of the locations in their home at least once for their remote communications across the three contexts.

In all contexts, most participants (WFH: 123/150, SFH: 178/208, LFH: 91/114) were comfortable with the locations of their meetings (see Figure 6) while having significant differences across the contexts. The regression analysis showed that compared to WFH, participants were significantly more
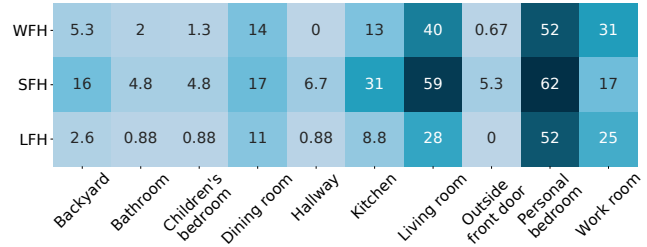

	Backyard	Bathroom	Children's bedroom	Dining room	Hallway	Kitchen	Living room	Outside front door	Personal bedroom	Work room
WFH	5.3	2	1.3	14	0	13	40	0.67	52	31
SFH	16	4.8	4.8	17	6.7	31	59	5.3	62	17
LFH	2.6	0.88	0.88	11	0.88	8.8	28	0	52	25

Figure 5: Usage of home locations (in percentage) reported by participants who engaged in remote communication contexts.
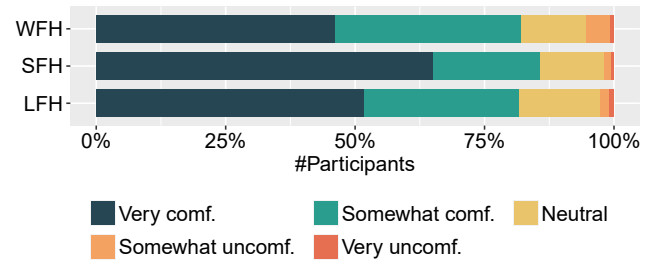

Figure 6: Participants' reported comfort level with frequently-used meeting locations.

comfortable when using any given location for their remote personal meetings (estimate $= 1.62$, p-value < 0.001).

4.4.1 Remote Privacy vs. Co-Inhabitant Privacy

In all three contexts, several participants reported to select a meeting location which they perceived to be the most private in their homes. Especially, in WFH, having privacy was the most frequently mentioned reason as to why a location is used for work meetings (WFH: 42/147). In the contexts of LFH and SFH, privacy was the second and third most common reason for participants' location-related decision making, respectively (LFH: 24/114, SFH: 35/208). Moreover, we found privacy and sense of safety to be frequently reported (WFH: 42/123, SFH: 68/178, LFH: 24/91) as participants' reasons to be comfortable with their meeting locations.

By qualitatively analyzing participants' open-ended responses, we identified two types of privacy: remote privacy and co-inhabitant privacy. Remote privacy refers to having privacy from other meeting attendees, while co-inhabitant privacy refers to having privacy from other household members. The types of privacy that were mentioned by participants varied among different contexts of remote communications.

In SFH, participants reported to have no concern over remote privacy as they felt comfortable with other meeting attendees (e.g., friends, family members) viewing their personal space. For example, P32 reported why they feel comfortable holding their personal meetings in the living room: "It's my living room, it's organized and everyone I talk to already knows it."

Almost all participants who considered privacy when se-

lecting their SFH meeting locations reported to be concerned with their co-inhabitant privacy. These participants reported to choose their meeting locations to be a personal space in their home where they are not being disturbed or interrupted by others during their remote meetings. Participants' personal space was mostly reported to be their bedroom. A few participants reported to have co-inhabitant privacy in other locations, including living room, kitchen, and workroom. P185 reported to use their bedroom for SFH meetings: "I feel the most comfortable in my own bedroom and I know that it will be a private space and that the least amount of interruptions will happen in my bedroom compared to other areas of the house." P25 reported why they were using the living room for personal meetings: "It is separated from the room in which my housemate works and so less likely that he will overhear."

Unlike SFH, in the contexts of WFH and LFH, participants' perception of privacy was more diverse. Some participants (WFH: 19/42, LFH: 15/24) reported to prefer having co-inhabitant privacy by detaching their meeting locations from other household members. P47 discussed why they decided to use their bedroom for remote work-related meetings: "I prefer using mostly my bedroom for most of my online work/meetings as I don't like others hearing me talk, I like to have a little bit of 'privacy'." P43 reported using their bedroom to preserve their co-inhabitant privacy: "I like to have my own little space, a bit of privacy from the rest of family and less distractions around so I can focus on the course." On the other hand, some participants were uncomfortable about others on the call seeing their personal space. These participants reported to desire having remote privacy by selecting a less personal location that provides a "neutral" or "professional" background with fewer details about their personal life. P195 talked about having privacy when holding their work meetings in the study or workroom: "I don't have anything private there that I would be unprofessional if I had to share my webcam with others." P122 discussed why they were using the kitchen for remote learning meetings: "This is the least personal place in the house to have such meetings."

Open-ended responses revealed potential conflicts between remote privacy and co-inhabitant privacy. In all contexts, participants who valued their co-inhabitant privacy frequently reported to be using their personal bedroom to have privacy from their household members. At the same time, participants in WFH and LFH perceived their personal bedrooms to be intimate and, therefore, not appropriate to preserve their remote privacy. We found similar tensions with regard to using living room for remote communications. Some participants chose to hold their remote meetings in the living room to have remote privacy, although having less co-inhabitant privacy due to the interruptions by household members.

4.4.2 Room Convenience and Equipment

Similar to participants' attitudes toward conferencing tools, convenience and comfort were frequently mentioned as

the deciding factor when selecting a meeting location (WFH: 26/147, SFH: 65/208, LFH: 24/114). Especially, in the context of SFH, participants reported that the convenience of the location is the most important reason when choosing the room for their remote personal meetings. P80 discussed why they use the living room for their personal meetings: "This is the location of relaxation and the area where my husband and I can sit comfortably and talk to friends and family."

Another commonly mentioned reason behind participants' choice of meeting location in all three contexts was the presence of equipment that was needed for remote communications, including computer, desk, and books (WFH: 42/147, SFH: 41/208, LFH: 37/114). For participants in the context of LFH, the room equipment was the main factor in deciding what room to use for their learning meetings. P75, who reported to use their bedroom for LFH meetings, said: "This is the location where I have my desk and my PC in."

4.4.3 Discomfort with Meeting Locations

Although most participants were comfortable with their selected meeting locations, some respondents reported to be somewhat or very uncomfortable (WFH: 9/150, SFH: 4/208, LFH: 3/114). Across all contexts, the main factor participants mentioned that made them uncomfortable with a location was the perceived invasion of remote/co-inhabitant privacy when holding meetings there (WFH: 4/9, SFH: 1/4, LFH: 2/3). In the LFH context, P115 reported that they are uncomfortable with using their bedroom for remote learning-related meetings: "It is hard to get comfortable in the bedroom as it feels like a private area to invite people in to." P4 discussed their discomfort with using the living room for their remote work meetings: "I could be overheard and am not comfortable with the webcam being on as it intrudes on my privacy."

The open-ended responses indicated that only participants in the WFH context took steps to mitigate their discomfort with the location of their meetings, while in the contexts of SFH and LFH, participants reported to take no action when being uncomfortable with their remote meeting locations. The primary approach participants mentioned to take in the context of WFH was to limit the information exposure, either to other meeting attendees or their household members (WFH: 3/9). P38, who reported to mainly use their living room for their work-related meetings, said: "I minimise what can be seen and test the audio quality before the meeting." Similarly, P35 limited the work-related information from the household members: "I close my door and ask other family members [not to] come to the living room when having work meetings."

5 Discussion

We first provide a brief comparison between the contexts of remote communications. Based on our findings, we then discuss methods to inform and enable users' privacy-protective decision making related to remote communications.

5.1 Context-Specific Privacy Concerns and Attributes

We focused on three remote communication contexts: working from home (WFH), socializing from home (SFH), and learning from home (LFH). In each context, we surfaced participants' attitudes and concerns toward the use of remote communication technologies. Our quantitative and qualitative findings suggested several similarities and differences in participants' attitudes, behaviors, and privacy concerns among the three contexts. In all contexts, comfort and discomfort with conferencing tools and meeting locations were mainly explained by participants' privacy and security concerns and their perceived sense of safety. Our findings indicated that WFH and LFH were similar in terms of the choice and the use of conferencing tools (e.g., activating webcam/microphone). In SFH, unlike other contexts, the decisions toward the conferencing tools and the meeting locations were primarily based on the provided convenience.

Numerous articles have been published that provide recommendations on how to better protect privacy when engaging in remote communications [39, 41, 84]. Almost all of these guidelines are targeted toward the users, who are already struggling with an insurmountable mental pressure thanks to the pandemic. When an awkward incident happens in a conference call, end users are not the only group to blame, as they are only a small part of the remote communication ecosystem. Tool developers and users' employers and educators could play a critical role in informing and empowering users to adopt privacy-protective behaviors while communicating with others online.

The pandemic may not last forever, but remote communications will stay longer [16] and that requires us to critically examine what we have learned during the pandemic. Based on our findings, in the following, we distill several recommendations to inform and empower users, and to design more privacy-protective tools.

5.2 Enabling Context-Specific Informed Decision Making

Participants' open-ended responses showed lack of autonomy in their attitudes and behaviors toward remote communication technologies. Several participants reported to have no control over the choice of conferencing tools for their WFH and LFH meetings (see Section 4.2.1). Lack of active decision making was also apparent in participants' attitudes toward the use of webcam and microphone. Participants reported to be explicitly (WFH and LFH) or implicitly (SFH) expected to turn on/off their webcam/camera in the meetings (see Section 4.3.2). The qualitative findings indicated that having limited or no control over the conferencing tools and their features (e.g., webcam/microphone) was participants' primary impediment to managing their tool-related privacy and security concerns (see Section 4.2.4). To enable active

and informed decision making in remote communications, we need to consider the context of the meeting.

Our findings suggested that WFH and LFH meetings have similar power dynamics that are being set by an authority figure (e.g., employer, educator). By providing **inclusive, transparent, and flexible policies**, workplaces and education institutes can take the first step toward informing and empowering meeting participants. To be inclusive, policies should acknowledge users' diverse and context-specific privacy needs and attitudes. To provide holistic privacy-protective policies, future studies should be conducted to explore other stakeholders' perspectives of remote communications, including but not limited to, employers and teachers.

In light of our findings, organizational policies need to discuss the choice of conferencing tool, the use of microphone and webcam in the meetings, and the available user controls. In addition, the policies should be flexible and open for feedback to help meeting attendees discuss and manage their concerns and discomfort. Items to be outlined in such policies include:

- What conferencing tools should be used for the meetings and why?
- What privacy and security controls are provided by the tools?
- In what condition are users (not) required to use their microphone/webcam?
- How can users control their microphone/webcam in the communication tools?
- How can meeting participants manage their concerns and discomfort with the tools?

Compared to WFH and LFH, in the context of SFH, participants felt being more in control of choosing a conferencing tool, which might be partially due to more balanced power dynamics. However, because of the implicit expectations, several participants felt having no control over the decision to activate their webcam/microphone in the personal meetings. As recommended by a few of our participants, **joint decision making** prior to the meeting could give meeting participants the opportunity to discuss their concerns and decide on a policy that accommodates and respects all of them.

5.3 Inclusive Privacy by Design

Across all contexts, the main factor participants mentioned to make them uncomfortable with a meeting location was the lack of remote and co-inhabitant privacy they felt when holding remote meetings in that location (see Section 4.4.1). Participants who referred to remote privacy reported that they do not feel comfortable having their home locations in the background of their WFH and LFH meetings. On the other hand, having a neutral or generic background was one of the frequently mentioned factors to make participants comfortable when using a meeting location (see Section 4.4.1).

Due to the restrictions posed by the diverse working, living, and learning arrangements, it may not be reasonable to ask everyone to find a neutral background for their remote meetings. Tool developers can enable features to help users protect their privacy. Some of the current communication tools, such as Zoom [85] and Microsoft Teams [86], already allow users to cover their real background by using virtual ones. Similarly, tools such as Skype [87] and Google Meet [88] provide a feature for users to blur their backgrounds.

Across all contexts, when discussing co-inhabitant privacy, several participants reported to be uncomfortable with other household members hearing their conversations (see Section 4.4.1). From the regression analysis, we found that an increase in the number of household members leads to a significant decrease in the level of comfort with conferencing tools as well as the locations of remote communications (see Table 1). To protect people's privacy in different contexts of remote communications, we need to design for diverse household settings. For example, to preserve co-inhabitant privacy in crowded settings, future remote communication devices can be enabled with a feature to detect and notify the user whether other household members are in the hearing range of their remote meetings. Such features can also respect the privacy needs of other meeting attendees, e.g., in case meeting participants are not comfortable with their voice or video being heard or seen by individuals who are not part of the call (e.g., household members).

5.4 Limitations

As the first paper to study remote communications at the transition of the pandemic, we surfaced participants' attitudes, behaviors, and concerns toward specific aspects of remote communications in different contexts. Due to the focus of our research and the survey methodology, we did not explore other potentially informative research questions, which could be studied in the future. In what follows, we will highlight the limitations of the current work, alongside several future research directions.

Our study used Prolific to recruit survey participants. Prior work recommended using Prolific to recruit a diverse sample of participants [89]. However, despite its diverse population and similarly to other crowdsourcing platforms, Prolific participants are not representative of any average population. For example, in Prolific, participants tend to be younger and more educated [90]. In addition, our participants were mainly from the UK, Poland, and the US, and we had a small number of participants from other countries (see Table 5). Due to these limitations, the findings of our study should not be generalized. Our study provides an overview of technology-related perceptions and behaviors during the global COVID-19 pandemic and we believe future studies can more directly focus on specific populations. In our study, participants' country of residence was not a statistically significant factor, which might be due to the small number of participants from some

of the countries. Future studies could explore the difference in privacy concerns and attitudes among different countries and cultures.

As we previously mentioned, among other questions, our survey explored how participants' learning experience has been impacted by the COVID-19 pandemic. In this study, we only recruited participants who were at least 18 years old. However, it is also important to understand the impact of the pandemic and the privacy considerations of students from all ages, which should be considered in a future study.

To ensure participants' familiarity with the contexts of remote communications, for each context, we only asked the survey questions of participants who reported to have familiarity with that specific context. This potential selection bias might impact participants' attitudes and concerns toward remote communications in each context. Similarly, due to the nature of the job and depending on the level of experience, crowd-source participants might be more familiar with remote communication technologies than the average population. Having familiarity with a technology has been shown to decrease the amount of risk an individual would perceive related to that technology [79]. Therefore, the reported privacy and security concerns captured by our study could be lower than the average population' risk perception toward remote communications.

6 Conclusion

The COVID-19 pandemic has caused people around the world to abruptly shift their in-person work, personal life, and/or education meetings to remote ones, which could outlast the pandemic. Therefore, to enable safe remote experience, it is critical to design privacy-protective tools and empower users to consider privacy and security when engaging in remote communications. To this end, we conducted a 220-participant survey on Prolific, in which we considered three contexts of remote communications, namely working (WFH), socializing (SFH), and learning from home (LFH). Our quantitative and qualitative findings indicated that concerns, attitudes, and behaviors toward remote communications are diverse and context-dependent. Across all contexts, privacy and security were among the most frequently mentioned concerns that participants had. These concerns were exacerbated by the fact that participants felt that they had no agency over decision making about conferencing tools and the modes of remote communications. We provided several recommendations for tool developers and organizations to enable users to make privacy- and security-protective choices when engaging with remote communications.

Acknowledgments

References

[1] Los Angeles Times, "Coronavirus social distancing around the world," https://www.latimes.com/world-nation/story/2020-04-06/coronavi-social-distancing-around-the-world, April 2020.

[2] R. Picheta, "Boris Johnson issues stay-at-home order, sending UK into lockdown to fight coronavirus pandemic," https://www.cnn.com/2020/03/23/uk/uk-coronavirus-lockdown-gbr-intl/index.html, accessed: 2020-10-28.

[3] M. Smith, "China forces millions of people to stay at home as virus toll rises," https://www.afr.com/world/asia/china-forces-millions-of-people-to-stay-at-home-as-virus-toll-rises-20200216-p5419e, accessed: 2020-10-28.

[4] The Washington Post, "Washington Post-ABC News poll March 22-25, 2020," https://www.washingtonpost.com/context/washington-post-abc-news-poll-march-22-25-2020/974c3312-5a40-4764-afb1-4bb6b86f1cf4/?itid=lk_inline_manual_2&itid=lk_inline_manual_2, accessed: 2020-10-28.

[5] D. Thompson, "The coronavirus is creating a huge, stressful experiment in working from home," https://www.theatlantic.com/ideas/archive/2020/03/coronavirus-creating-huge-stressful-experiment-working-home/607945/, March 2020.

[6] E. Koeze and N. Popper, "The virus changed the way we internet," https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html, April 2020.

[7] A. Tugend, P. Jordan, and M. Stein, "This school year has been unlike any other," https://www.nytimes.com/2020/10/14/education/learning/pandemic-school-remote-learning.html, October 2020.

[8] N. Daniels, "When the Pandemic Ends, Will School Change Forever?" https://www.nytimes.com/2020/05/05/learning/when-the-pandemic-ends-will-school-change-forever.html, May 2020.

[9] P. Wagenseil, "Zoom security issues: Here's everything that's gone wrong (so far)," https://www.tomsguide.com/news/zoom-security-privacy-woes, November 2020.

[10] Z. Doffman, "Why You Should Stop Sending Links On Facebook Messenger," https://www.forbes.com/sites/zakdoffman/2020/10/25/why-apple-iphone-and-google-android-users-should-stop-using-facebook-messenger-apps/?sh=1811fd9c33f1, accessed: 2020-10-28.

[11] C. Mihalcik, "Microsoft listened to Skype calls with 'no security' to protect recordings, report says," https://www.cnet.com/news/microsoft-listened-to-skype-calls-with-no-security-to-protect-recordings-report-says/, accessed: 2020-10-28.

[12] R. Perper, "WhatsApp disclosed 12 security flaws last year, including 7 classified as 'critical,' after Jeff Bezos phone was reportedly hacked," https://www.businessinsider.com/jeff-bezos-hack-whatsapp-disclosed-security-flaws-last-year-ft-2020-1, accessed: 2020-10-28.

[13] Zoom, "Attendee attention tracking," https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking, accessed: 2020-10-28.

[14] B. Fung and A. Marquardt, "Millions of americans are suddenly working from home. that's a huge security risk," https://www.cnn.com/2020/03/20/tech/telework-security/index.html, March 2020.

[15] M. Liberman, "Massive shift to remote learning prompts big data privacy concerns," https://www.edweek.org/technology/massive-shift-to-remote-learning-prompts-big-data-privacy-concerns/2020/03, March 2020.

[16] M. Brenan, "U.S. Workers Discovering Affinity for Remote Work," https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx, April 2020.

[17] Prolific, "Quickly find research participants you can trust." https://www.prolific.co/, accessed: 2020-11-26.

[18] P. Emami-Naeini, T. Francisco, T. Kohno, and F. Roesner, "Understanding privacy attitudes and concerns towards remote communications during the COVID-19 pandemic," *arXiv preprint arXiv:2106.05227*, 2021.

[19] S. O'Grady, K. Bellware, M. Iati, L. Beachum, H. Denham, R. Thebault, and D. Sands, "The coronavirus has killed at least 1 million people worldwide," https://www.washingtonpost.com/nation/2020/09/28/coronavirus-covid-live-updates-us/, September 2020.

[20] Centers for Disease Control and Prevention (CDC), "Social Distancing," https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/social-distancing.html, accessed: 2020-10-28.

[21] D. G. Hayward, *Home as an environmental and psychological concept*, 1975.

[22] C. Trueman, "Pandemic leads to surge in video conferencing app downloads," https://www.computerworld.com/article/3535800/pandemic-leads-to-surge-in-video-conferencing-app-downloads.html, April 2020.

[23] J. Novet, "Why Zoom has become the darling of remote workers during the COVID-19 crisis," https://www.cnbc.com/2020/03/21/why-zoom-has-become-darling-of-remote-workers-amid-covid-19-outbreak.htmll, accessed: 2020-10-28.

[24] M. Hachman, "Microsoft's solution for COVID-19 is a free Teams subscription for six months," https://www.pcworld.com/article/3530374/microsofts-solution-for-covid-19-is-a-free-teams-subscription-for-six-months.html, accessed: 2020-10-28.

[25] I. Bonifacic, "Google makes Hangouts Meet features free in the wake of coronavirus," https://www.engadget.com/2020-03-03-google-makes-hangouts-meet-features-free-in-the-wake-of-coronavirus.html, accessed: 2020-10-28.

[26] J. Novet, "Cisco says Webex video-calling service is seeing record usage too, even as competitor Zoom draws all the attention," https://www.cnbc.com/2020/03/17/cisco-webex-sees-record-usage-during-coronavirus-expansion-like-zoom.html, accessed: 2020-10-28.

[27] T. Lorenz, "'zoombombing': When video conferences go wrong," https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html, accessed: 2020-10-28.

[28] A. Krolik and N. Singer, "A feature on Zoom secretly displayed data from people's LinkedIn profiles," https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html, accessed: 2020-10-28.

[29] J. Rosenblatt, "Zoom sued for allegedly illegally disclosing personal data," https://www.bloomberg.com/news/articles/2020-03-31/zoom-sued-for-allegedly-illegally-disclosing-personal-data, accessed: 2020-10-28.

[30] T. C. Li, "Privacy in pandemic: Law, technology, and public health in the covid-19 crisis," 2020.

[31] S. Bassan, "Data privacy considerations for telehealth consumers amid covid-19," *Journal of Law and the Biosciences*, vol. 7, no. 1, p. lsaa075, 2020.

[32] C. Venzke, "For remote learning, privacy challenges go beyond zoombombing," https://cdt.org/insights/for-remote-learning-privacy-challenges-go-beyond-zoombombing/, July 2020.

[33] S. Morrison and R. Heilweil, "How teachers are sacrificing student privacy to stop cheating," https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning, December 2020.

[34] J. Duball, "Shift to online learning ignites student privacy concerns," https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/, April 2020.

[35] C. Caron, "How to protect your family's privacy during remote learning," https://www.nytimes.com/2020/08/20/parenting/online-school-privacy.html, August 2020.

[36] V. Strauss, "As schooling rapidly moves online across the country, concerns rise about student data privacy," https://www.washingtonpost.com/education/2020/03/20/schooling-rapidly-moves-online-across-country-concerns-rise-about-student-data-privacy/, March 2020.

[37] T. Spiggle, "Can employers monitor employees who work from home due to the coronavirus?" https://www.forbes.com/sites/tomspiggle/2020/05/21/can-employers-monitor-employees-who-work-from-home-due-to-the-coronavirus/?sh=3a31c6202fb7, May 2020.

[38] S. Morrison, "Just because you're working from home doesn't mean your boss isn't watching you," https://www.vox.com/recode/2020/4/2/21195584/coronavirus-remote-work-from-home-employee-monitoring, April 2020.

[39] V. Safronova, "Digital hygiene in the Zoom era," https://www.nytimes.com/2020/10/22/style/zoom-safety-protocols.html, October 2020.

[40] J. Engel Bromwich, "Protecting your digital life in 9 easy steps," https://www.nytimes.com/2016/11/17/technology/personaltech/encryption-privacy.html, November 2016.

[41] H. Drew, "How to protect your Zoom calls," https://www.washingtonpost.com/technology/2020/04/03/zoom-video-set-up/, April 2020.

[42] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[43] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy expectations and preferences in an iot world," in *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, 2017, pp. 399–412.

[44] D. Howley, "Americans buying 'historic' amount of computers during coronavirus lockdown," https://finance.yahoo.com/news/americans-buying-historic-amount-computers-webcams-121043910.html, April 2020.

[45] C. Welch, "Webcams have become impossible to find, and prices are skyrocketing," https://www.theverge.com/2020/4/9/21199521/webcam-shortage-price-raise-logitech-razer-amazon-best-buy-ebay, April 2020.

[46] C. Baraniuk, "No end to covid-19 webcam shortage," https://www.bbc.com/news/technology-53506401, July 2020.

[47] B. Hill, "The covid-19 pandemic has caused a webcam shortage, and street prices are soaring," https://hothardware.com/news/covid-19-webcam-shortage-prices-skyrocketing, April 2020.

[48] J. Stern, "What i learned from the hacker who spied on me," https://www.wsj.com/articles/what-i-learned-from-the-hacker-who-spied-on-me-11549559728, February 2019.

[49] C. Williams, "Risk: Is this your webcam? you're being watched," https://www.wizcase.com/blog/webcam-security-research/, September 2019.

[50] M. Kuma, "Mac malware can secretly spy on your webcam and mic – here's how to stay safe," https://thehackernews.com/2016/10/macbook-camera-hacked.html, October 2016.

[51] K. O'Flaherty, "Zoom users beware: Here's how a flaw allows attackers to take over your mac microphone and webcam," https://www.forbes.com/sites/kateoflahertyuk/2020/04/01/zoom-users-beware-heres-how-a-flaw-allows-attackers-to-take-over-your-mac-microphone-and-webcam/?sh=7b2fe9e22fbe, April 2020.

[52] K. Johnson, "Ohio man charged for remotely controlling devices, spying on people for 13 years," https://www.usatoday.com/story/news/politics/2018/01/10/ohio-man-charged-remotely-controlling-devices-spying-people-13-years/1022275001/, January 2018.

[53] G. Kumparak, "Nasty facetime bug could allow others to eavesdrop on your microphone or camera," https://techcrunch.com/2019/01/28/nasty-facetime-bug-could-allows-others-to-eavesdrop-on-your-microphone-or-camera/, January 2019.

[54] H. Coffey, "Is it safe to leave your webcam uncovered after using video chat apps?" https://www.independent.co.uk/life-style/webcam-zoom-privacy-safety-tech-security-hack-working-home-lockdown-a9469156.html, April 2020.

[55] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner, "Somebody's watching me? assessing the effectiveness of webcam indicator lights," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 1649–1658.

[56] M. Brocker and S. Checkoway, "iseeyou: Disabling the macbook webcam indicator {LED}," in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 337–352.

[57] G. Cluley, "Webcam spying without turning on the led? researchers prove it's possible," https://grahamcluley.com/webcam-spying-without-turning-led-researchers-prove-possible/, December 2013.

[58] T. Germain, "How to protect yourself from camera and microphone hacking," https://www.consumerreports.org/privacy/how-to-protect-yourself-from-camera-and-microphone-hacking/, July 2019.

[59] D. Cook, "Zoom, skype, microsoft teams: Why you should cover the camera on your phone or laptop," https://nationalpost.com/news/canada/hackers-can-access-your-phone-and-laptop-cameras-heres-why-you-should-cover-them-now, April 2020.

[60] D. Safreno, "Loneliness is distracting," https://pragli.com/blog/loneliness-is-distracting/, March 2020.

[61] M. Jagannathan, "Like 'punching a time clock through your webcam': How employers are keeping tabs on remote workers during the pandemic," https://www.marketwatch.com/story/like-punching-a-time-clock-through-your-webcam-how-employers-are-keeping-tabs-on-remote-workers-during-the-pandemic-11596484344, August 2020.

[62] A. Holmes, "Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working — and the service is seeing a rapid expansion since the coronavirus outbreak," https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3, March 2020.

[63] D. West, "How employers use technology to surveil employees," https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/, January 2021.

[64] P. Cohen and T. Hsu, "'rolling shock' as job losses mount even with reopenings," https://www.nytimes.com/2020/05/14/business/economy/coronavirus-unemployment-claims.html, June 2020.

[65] G. Genhart, "Spying on students: School-issued devices and student privacy," https://www.eff.org/wp/school-issued-devices-and-student-privacy, April 2017.

[66] D. Harwell, "Cheating-detection companies made millions during the pandemic. now students are fighting back." https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/, November 2020.

[67] R. Deibert, "We've become dependent on a technological ecosystem that is highly invasive and prone to serial abuse," https://www.theglobeandmail.com/opinion/article-the-pandemic-has-made-us-even-more-dependent-on-a-highly-invasive/, November 2020.

[68] S. Johnson, "On or off? california schools weigh webcam concerns during distance learning," https://edsource.org/2020/on-or-off-california-schools-weigh-webcam-concerns-during-distance-learning/638984, August 2020.

[69] W. D. Perreault, "Controlling order-effect bias," *The Public Opinion Quarterly*, vol. 39, no. 4, pp. 544–551, 1975.

[70] T. Fernandez, A. Godwin, J. Doyle, D. Verdin, H. Boone, A. Kirn, L. Benson, and G. Potvin, "More comprehensive and inclusive approaches to demographic data collection," 2016.

[71] C. M. Steele, "A threat in the air: How stereotypes shape intellectual identity and performance." *American psychologist*, vol. 52, no. 6, p. 613, 1997.

[72] S. J. Spencer, C. M. Steele, and D. M. Quinn, "Stereotype threat and women's math performance," *Journal of experimental social psychology*, vol. 35, no. 1, pp. 4–28, 1999.

[73] J. Saldaña, *The coding manual for qualitative researchers*. Sage, 2015.

[74] E. Namey, G. Guest, L. Thairu, and L. Johnson, "Data reduction techniques for large qualitative data sets," *Handbook for team-based qualitative research*, vol. 2, no. 1, pp. 137–161, 2008.

[75] J. L. Fleiss, B. Levin, and M. C. Paik, *Statistical methods for rates and proportions*. John Wiley & Sons, 2013.

[76] K. P. Burnham and D. R. Anderson, "Multimodel inference: understanding AIC and BIC in model selection," *Sociological methods & research*, vol. 33, no. 2, pp. 261–304, 2004.

[77] E. Zeng and F. Roesner, "Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 159–176.

[78] P. Oppmann, "In digital world, we trade privacy for convenience," https://www.cnn.com/2010/TECH/04/14/oppmann.off.the.grid/index.html, April 2010.

[79] E. U. Weber, N. Siebenmorgen, and M. Weber, "Communicating asset risk: How name recognition and the format of historic volatility information affect risk perception and investment decisions," *Risk Analysis: An International Journal*, vol. 25, no. 3, pp. 597–609, 2005, accessed: 2020-06-03.

[80] R. B. Cialdini and N. J. Goldstein, "Social influence: Compliance and conformity," *Annu. Rev. Psychol.*, vol. 55, pp. 591–621, 2004.

[81] M. Deutsch and H. B. Gerard, "A study of normative and informational social influences upon individual judgment." *The journal of abnormal and social psychology*, vol. 51, no. 3, p. 629, 1955.

[82] C. Heath, R. P. Larrick, and J. Klayman, "Cognitive repairs: How organizational practices can compensate for individual shortcomings," in *Review of Organizational Behavior*. Citeseer, 1998.

[83] M. Sherif, "A study of some social factors in perception." *Archives of Psychology (Columbia University)*, 1935.

[84] B. Chen, "The Dos and Don'ts of Online Video Meetings," https://www.nytimes.com/2020/03/25/technology/personaltech/online-video-meetings-etiquette-virus.html, March 2020.

[85] Zoom, "Virtual Background," https://support.zoom.us/hc/en-us/articles/210707503-Virtual-Background, 2020, accessed: 2020-11-21.

[86] J. Spataro, "Custom backgrounds in Microsoft Teams make video meetings more fun, comfortable, and personal," https://www.microsoft.com/en-us/microsoft-365/blog/2020/06/12/custom-backgrounds-microsoft-teams-video-meetings-fun-comfortable-personal/, June 2020.

[87] Team Skype, "Introducing background blur in Skype," https://www.skype.com/en/blogs/2019-02-background-blur/, June 2019.

[88] Google, "Blur your background in Google Meet," https://workspaceupdates.googleblog.com/2020/09/blur-your-background-in-google-meet.html, September 2020.

[89] E. Peer, L. Brandimarte, S. Samat, and A. Acquisti, "Beyond the turk: Alternative platforms for crowdsourcing behavioral research," *Journal of Experimental Social Psychology*, vol. 70, pp. 153–163, 2017.

[90] Prolific Team, "What are the advantages and limitations of an online sample?" https://researcher-help.prolific.co/hc/en-gb/articles/360009501473-What-are-the-advantages-and-limitations-of-an-online-sample-, September 2018.

A Survey Questions

A.1 Informed Consent

This is a survey about technology use in the home during the Coronavirus (COVID-19) pandemic by researchers at the University of Washington, in Seattle, Washington, USA. The University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm.

In order to participate, you must be at least 18 years old and able to complete the survey in English. We expect this survey will take about 20 minutes to complete. If you have any questions about this survey, you may email us at hometechnology@cs.washington.edu.

- I am 18 years or older.
  ○ Yes ○ No

- I have read and understand the information above.
  ○ Yes ○ No

- I want to participate in this research and continue with the task.
  ○ Yes ○ No

A.2 Context-Specific Questions (CQ)

In the contexts of WFH, SFH, and LFH, we referred to remote communications as "remote work-related meetings," "remote personal meetings with friends and family members," and "remote learning-related meetings," respectively. Here we only provide the questions for the WFH context.

- **CQ1:** Have you been mostly having remote work-related meetings from home during the COVID-19 pandemic?
  ○ Yes ○ No

  The rest of the context-related questions will only be presented if the answer is "Yes."

- **CQ2:** Before the COVID-19 pandemic, how often have you had remote work-related meetings from home?
  ○ Never ○ Once or twice a year ○ Once every 4-6 months ○ Once every 2-3 months ○ Once every month ○ Once every 2-3 weeks ○ Once every week ○ Not every day, but more than once a week ○ Every day

- **CQ3:** During the COVID-19 pandemic, how many hours a week do you spend in remote work-related meetings from home?
  ○ Less than 1 ○ 1 to 5 hours ○ 6 to 10 hours ○ 11 to 15 hours ○ 16 to 20 hours ○ 21 to 25 hours ○ 26 to 30 hours ○ 31 to 35 hours ○ 36 to 40 hours ○ Over 40 hours

- **CQ4:** During the COVID-19 pandemic, how long have you been having remote work-related meetings from home?
  ○ Since last week ○ Since two weeks ago ○ Since three weeks ago ○ Since one month ago ○ Since more than one month ago

- **CQ5:** During the COVID-19 pandemic, what conferencing tools do you mostly use for your remote work-related meetings? If you use more than one tool, please select the one you use most frequently.
  ○ BlueJeans ○ Google Hangouts ○ Google Meet ○ GoToMeeting ○ Microsoft Teams ○ Skype ○ Slack ○ UberConference ○ Zoom ○ Other (please specify [Open-ended])

- **CQ6:** Please explain why you have been using the tool that you have specified more frequently than other tools. [Open-ended]

- **CQ7:** During the COVID-19 pandemic, in your current environment, how do you feel about using this tool for your remote work-related meetings?
  ○ Very uncomfortable ○ Somewhat uncomfortable ○ Neither uncomfortable nor comfortable ○ Somewhat comfortable ○ Very comfortable

- **CQ8:** *(If in CQ7, Very uncomfortable or Somewhat uncomfortable is selected)* What about this tool makes you uncomfortable when using it? [Open-ended]

- **CQ9:** *If in CQ7, Very uncomfortable or Somewhat uncomfortable is selected)* How do you manage your discomfort when using this tool? [Open-ended]

- **CQ10:** *If in CQ7, Very comfortable or Somewhat comfortable is selected)* What about this tool makes you comfortable when using it? [Open-ended]

- **CQ11:** During the COVID-19 pandemic, how often do you turn on your device's webcam when having remote work-related meetings?
  ○ Never   ○ Rarely   ○ Sometimes   ○ Frequently   ○ Always

- **CQ12:** How do you decide whether or not to turn on your device's webcam when having remote work-related meetings? [Open-ended]

- **CQ13:** During the COVID-19 pandemic, how often do you turn on your device's microphone when having remote work-related meetings?
  ○ Never   ○ Rarely   ○ Sometimes   ○ Frequently   ○ Always

- **CQ14:** How do you decide whether or not to turn on your device's microphone when having remote work-related meetings? [Open-ended]

- **CQ15:** During the COVID-19 pandemic, which area of your home do you usually hold your remote work-related meetings in? If you use more than one location, please select the one you use most frequently for remote work-related remote meetings.
  ○ Backyard   ○ Bathroom   ○ Bedroom (yours)   ○ Bedroom (your children's)   ○ Dining room   ○ Hallway   ○ Kitchen   ○ Living room   ○ Outside front door   ○ Study or workroom   ○ Other (please specify [Open-ended])

- **CQ16:** During the COVID-19 pandemic, how do you feel about using this location to have remote work-related meetings?
  ○ Very uncomfortable   ○ Somewhat uncomfortable   ○ Neither uncomfortable nor comfortable   ○ Somewhat comfortable   ○ Very comfortable

- **CQ17:** *(If in CQ16, Very uncomfortable or Somewhat uncomfortable is selected)* What about this location makes you uncomfortable when having remote work-related meetings there? [Open-ended]

- **CQ18:** *If in CQ16, Very uncomfortable or Somewhat uncomfortable is selected)* How do you manage your discomfort when using this location for having remote work-related meetings? [Open-ended]

- **CQ19:** *If in CQ16, Very comfortable or Somewhat comfortable is selected)* What about this location makes you comfortable when having remote work-related meetings there? [Open-ended]

- **CQ20:** During the COVID-19 pandemic, have you or people you know ever experienced an awkward incident while having remote work-related meetings?
  ○ Yes   ○ No

- **CQ21:** *(If in CQ18, Yes is selected)* Please describe the incident. [Open-ended]

- **CQ22:** *(If in CQ18, Yes is selected)* Please describe what you or people you know have done in response to the incident. [Open-ended]

A.3   Demographics and Home Settings

- **DH1:** Including yourself, how many adults 18 years of age and above live in your current home?
  ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH2:** How many children at or above the age of 13 and under the age of 18 live in your current home?
  ○ 0   ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH3:** How many children at or above the age of 7 and under the age of 13 live in your current home?
  ○ 0   ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH4:** How many children under the age of 7 live in your current home?
  ○ 0   ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH5:** Who do you share your home with? (check as many as apply)
  ○ No one   ○ Roommate(s)   ○ Spouse(s)/Domestic partner(s)   ○ Children   ○ Parent(s)   ○ Other (please specify [Open-ended])

- **DH6:** Do you have shared wall(s) with your neighbors?
  ○ Yes   ○ No

- **DH7:** How many bedrooms does your home have?
  ○ 0   ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH8:** How many rooms other than bedrooms does your home have?
  ○ 0   ○ 1   ○ 2   ○ 3   ○ 4   ○ 5   ○ More than 5

- **DH9:** What is your age?
  ○ 18-29 years old   ○ 30-49 years old   ○ 50-64 years old   ○ 65 years and older

- **DH10:** What is your gender? [Open-ended]

- **DH11:** What is the highest degree you have earned?
  ○ No schooling completed   ○ Nursery school   ○ Grades 1 through 11   ○ 12th grade—no diploma   ○ Regular high school diploma   ○ GED or alternative credential   ○ Some college credit, but less than 1 year of college   ○ 1 or more years of college credit, no degree   ○ Associates degree (for example: AA, AS)   ○ Bachelor's

degree (for example: BA. BS) ○ Master's degree (for example: MA, MS, MEng, MEd, MSW, MBA) ○ Professional degree beyond bachelor's degree (for example: MD, DDS, DVM, LLB, JD) ○ Doctorate degree (for example: Ph.D., EdD)

- **DH12:** In which country do you currently reside? [List of countries provided by Qualtrics]

- **DH13:** What is your current employment status?
○ Full-time employment ○ Part-time employment ○ Unemployed ○ Self-employed ○ Home-maker ○ Student ○ Retired

- **DH14:** *(If in DH13, Unemployed or Retired is not selected)* The organization you work for is in which of the following?
○ Public sector (e.g., government) ○ Private sector (e.g., most businesses and individuals) ○ Non-for-profit sector

- **DH15:** Do you have a background in technology?
○ Yes ○ No

- **DH16:** *(If in DH14, Yes is selected)* Please specify what your technical background is. [Open-ended]

B Codebooks

The codebooks are available at:
https://gist.github.com/SOUPS-COVID-Privacy/97b6f6caeb13d5091314e6458049617d.

C Participants' Information

Timeline	Meeting Frequency	Context		
		WFH	SFH	LFH
Before the pandemic	Never	53%	33%	60%
	Once/twice a year	6%	7%	14%
	Once every 4-6 months	4%	6%	5%
	Once every 2-3 months	4%	7%	3%
	Once every month	3%	6%	2%
	Once every 2-3 weeks	4%	10%	2%
	Once every week	6%	13%	3%
	> once a week	11%	12%	5%
	Every day	9%	6%	6%
During the pandemic	< 1 (hour/week)	25%	35%	11%
	1-5 (hour/week)	44%	41%	40%
	6-10 (hour/week)	13%	14%	16%
	11-15 (hour/week)	7%	3%	12%
	16-20 (hour/week)	6%	2%	11%
	21-25 (hour/week)	1%	1%	7%
	26-30 (hour/week)	1%	1%	3%
	31-35 (hour/week)	2%	1%	0%
	36-40 (hour/week)	1%	1%	0%
	> 40 (hour/week)	0%	1%	0%

Table 2: Frequency of engaging in remote communications.

Experience Duration	Context		
	WFH	SFH	LFH
Since last week	1%	1%	7%
Since two weeks ago	0%	1%	5%
Since three weeks ago	3%	2%	9%
Since one month ago	5%	3%	18%
Since more than one month ago	91%	93%	61%

Table 3: Summary statistics of how long participants were experiencing the three contexts under study.

Question	Responses					
Shared wall(s) with neighbors	Yes	No				
	54%	46%				
Housemates	No one	Roommate(s)	Spouse(s)/Domestic partner(s)	Children	Parent(s)	Other: Siblings
	3%	3%	19%	11%	21%	25%
#Adults 18+ years old	1	2	3	4	5	More than 5
	12%	45%	22%	17%	4%	0%
#Children between 13 and 18 years old	0	1	2	3	4	5	More than 5
	81%	12%	6%	1%	0%	0%	0%
#Children between 7 and 13 years old	0	1	2	3	4	5	More than 5
	86%	14%	0%	0%	0%	0%	X%
#Children under 7 years old	0	1	2	3	4	5	More than 5
	83%	12%	5%	0%	0%	0%	0%
#Bedrooms	0	1	2	3	4	5	More than 5
	0%	14%	28%	41%	14%	3%	0%
#Rooms other than bedrooms	0	1	2	3	4	5	More than 5
	4%	11%	17%	27%	26%	15%	0%

Table 4: Breakdown of participants' home settings.

Age		Gender		Highest Degree		Country of Residence		Employment		Tech Background	
18-29	62%	Female	43%	No schooling completed	0%	UK	31%	Full-time	41%	Yes	35%
30-49	34%	Male	57%	Nursery school	0%	Poland	15%	Part-time	17%	No	65%
50-64	4%			Grades 1 through 11	2%	US	14%	Unemployed	6%		
				12th grade—no diploma	3%	Italy	7%	Self-employed	8%		
				Regular high-school diploma	21%	Portugal	7%	Home-maker	3%		
				GED or alternative credential	0%	Spain	4%	Student	25%		
				Some college credit, < 1 year of college	4%	Greece	3%	Retired	0%		
				1+ years of college credit, no degree	16%	Canada	2%	Public sector	23%		
				Associate's degree (e.g., AA, AS)	4%	Other	17%	Private sector	67%		
				Bachelor's degree (e.g., BA, BS)	37%			Non-profit sector	10%		
				Master's degree (e.g., MA, MS, MBA)	13%						
				Professional degree (e.g., MD, JD)	0%						
				Doctorate degree (e.g., Ph.D., EdD)	0%						

Table 5: Participants' demographic information. Only countries with at least 5 participants are listed.