# “I saw your partner naked”: Exploring Privacy Challenges During Video-based Online Meetings

Sarah Prange
sarah.prange@unibw.de
University of the Bundeswehr Munich
LMU Munich
Germany

Sarah Delgado Rodriguez
sarah.delgado@unibw.de
University of the Bundeswehr Munich
Germany

Lukas Mecke
lukas.mecke@unibw.de
University of the Bundeswehr Munich
LMU Munich
Germany

Florian Alt
florian.alt@unibw.de
University of the Bundeswehr Munich
Germany

## ABSTRACT

Video-based online meetings and, ultimately, the amount of private information that is shared – intentionally or accidentally – increased as a result of the COVID-19 pandemic. For example, online teaching might reveal lecturers’ private environment to students or business meetings might provide insights about employees’ family relationships. This raises the need to understand users’ perception towards privacy intrusion during online video conferences to inform concepts that better protect meeting participants’ privacy. We present the results of an online survey ($N = 140$) in which we investigate user stories of privacy-invasive situations in their homes during such meetings. Our results show that online meetings reveal private information that would not have become available during physical meetings. This often involves third parties (e.g., children, spouse, colleague), who might not even be aware of this. We discuss potential means to support users in protecting their and others’ privacy before, during, and after video-based online meetings.

## CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *User studies.*

## KEYWORDS

privacy, privacy mechanisms, online meetings, online meeting privacy, COVID-19

**ACM Reference Format:**
Sarah Prange, Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. “I saw your partner naked”: Exploring Privacy Challenges During Video-based Online Meetings. In *21th International Conference on Mobile and Ubiquitous Multimedia (MUM 2022), November 27–30, 2022, Lisbon, Portugal.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3568444.3568468

## 1 INTRODUCTION

The year 2020 witnessed a considerable shift of work-related activities from offices to users’ homes due to the COVID-19 pandemic. As a result of this, many activities that usually require users’ presence – that is meetings, courses, events, or conferences, to just name a few – moved to online formats. In a similar way, also leisure activities, such as meeting friends or family, shifted into the digital world. Although some of these activities are now being held in person again, there is still an increased number of online or hybrid events.

One way to facilitate this entails the use of video conferencing software to transmit a subset of real-world communication cues like vocal tone, mimics, and gestures. At the same time, this also provides communication partners a window into users’ private environments. As a result, personal information may leak incidentally, often without the user even knowing. Examples could include users’ musical abilities (due to a guitar in the background) but also their political views or sexual orientations. Furthermore, it is also possible that information about other (potentially unaware) users in the environment is revealed, for example, as children crash business meetings[1].

Current tools for video-based online meetings often do little to address this – both on a technical level as well as on a user-interface level. Examples of privacy protection measures for users include features that allow the image to be manipulated, such as blurring the background or applying filters to the user’s face. At the same time, such features might not be available in tools employees are required to use or features may not work very well for technical reasons (e.g., lighting or objects in the camera’s field of view). Furthermore, the effect of such measures is limited, as, for instance, filters often pose usability challenges (cf. a lawyer unable to remove the cat filter[2]) and applying blur is insufficient to protect users’ privacy as in turn awareness gets lost [25].

*MUM 2022, November 27–30, 2022, Lisbon, Portugal*

ACM ISBN 978-1-4503-9820-6/22/11…$15.00
https://doi.org/10.1145/3568444.3568468

*All sources last accessed June 3, 2022*

[1] https://edition.cnn.com/videos/business/2021/01/25/trivago-ceo-son-crashes-interview.cnnbusiness

[2] https://www.reuters.com/article/us-texas-hearing-cat-filter-idUSKBN2A935Q

We argue that in order to design means for users to better protect their privacy during video-based online meetings, a more fundamental understanding of potential privacy intrusion during such meetings is needed. We address this in our work by answering the following questions:

**RQ1** *What* privacy-relevant information about users is at risk during video-based online meetings?

**RQ2** *How* do video-based online meetings facilitate the leakage of such information?

**RQ3** What are possible means to *mitigate* this?

In particular, we conducted an online survey ($N = 140$) in which we collected user stories of online meetings during lockdowns in 2020. We asked participants to describe situations related to online meetings during lockdowns, in which information was revealed about either themselves or others.

We found speakers' webcam and/or audio stream frequently carrying privacy-relevant information such as hints at living situations, family relationships, or hobbies. While many participants took active measures to protect their privacy such as, e.g. searching for a neutral background within their home, these were not always effective, especially for spontaneous meetings. We conclude by discussing means to support users *before*, *during* and *after* video-based online meetings to preserve their as well as others' privacy.

## 2 BACKGROUND AND MOTIVATION

In 2020, around 100 countries faced national lockdown periods as a reaction to COVID-19[3]. During this time, users spent considerable amounts of time at home and many companies introduced remote working opportunities to their employees. This not only led to increased network traffic in general [13] but in particular to increased use of video conferencing software[4] for business as well as private purposes. Also, many events, including technology-related conferences[5], moved to online formats (e.g., the SOUPS conference 2020[6]). Hence, many researchers presented their work from home – be it through pre-recorded talks or live-streamed online events – and thus provided insights into their homes. For example, items in the background or unanticipated events revealed private information that would have stayed secret at a physical event, posing a challenge to speakers' privacy. Generally, users' *privacy* refers to their ability to decide and control their personal data being collected [7] and/or shared. However, this becomes challenging as computational systems are by now ubiquitous [37], and using online communication tools became increasingly indispensable during the pandemic.

### 2.1 Privacy at Home

The home is considered a private space by users [8]. However, recent advances in technology brought devices capable of collecting and processing – potentially sensitive – data to users' (smart) homes. This raises privacy concerns towards smart home devices [1, 33, 39]. In particular, users are concerned about illegitimate physical or remote access to their homes [41, 43].

With the increased use of video conferencing software, another channel for capturing private insights into users' homes has emerged. However, to the best of our knowledge, users' experiences of potential privacy intrusion arising from this have not been investigated so far. While users are willing to sacrifice their privacy and adapt smart home technology for convenience [11, 42], it is unclear whether this holds true for the use of video conferencing software at home.

### 2.2 COVID-19 Affecting Privacy and Security

During the pandemic, the use of online communication tools increased massively[7]. At the same time, the use of such communication tools puts users' security and privacy at risk [16]. Many of the common software options do not implement adequate means to protect both, security and privacy[8]. New cybersecurity threats emerged from the COVID-19 pandemic (e.g., recent spam exploits users' fear of the virus) [18]. Also, many network connections to users' home offices were unprotected, while cybercrime increased [2].

As a result, users were exposed to security and privacy risks a) without having a real choice, as there was a sudden need to move online, and/or b) without even being aware of it as popular video conferencing software collects more data than users are aware of[9]. Related work also identified an increased collection and sharing of personal data during the pandemic, as, e.g., health and location data is tracked and shared to identify effective countermeasures. Also, as many activities moved online, new digital records exist about users [4]. Particularly for video conferences, Kagan et al. showed that personal information can be identified using image processing techniques. In combination with social media data, users can be identified across online meetings [16]. Some governments even enforced the use of location-based applications to ensure adherence to quarantine regulations, leading users to (involuntarily) change routines and data sharing practices [38].

To summarize, the COVID-19 pandemic clearly put users' privacy at risk. While related work identified potential threats, we focus on *users' experiences* of privacy intrusion during video conferences.

## 3 ONLINE SURVEY: STAY HOME SITUATIONS

To capture users' experiences with online activities during the lockdown, we conducted an online survey between June and October 2020, asking for information that was (unintentionally) shared during video conferences (RQ1, RQ2). We also asked for privacy measures that participants did apply and whether they considered these to be effective (RQ3).

### 3.1 Questionnaire Structure

In line with related work, we started our survey with a general question on a situation that could be reported from both perspectives, victim and observer of privacy intrusion [9, 28]. We then asked a number of detail questions regarding the online meeting and participants' demographics. Hence, the questionnaire comprised three

[3] https://www.bbc.com/news/world-52103747

[4] https://www.statista.com/statistics/1109875/download-growth-video-conferencing-apps/

[5] https://www.statista.com/statistics/1105833/COVID-coronavirus-impact-tech-conferences/

[6] https://www.usenix.org/conference/soups2020/technical-sessions

[7] https://www.marketwatch.com/story/zoom-microsoft-cloud-usage-are-rocketing-during-coronavirus-pandemic-new-data-show-2020-03-30

[8] https://theconversation.com/videoconferencing-keeps-people-connected-while-the-coronavirus-keeps-them-inside-but-privacy-and-security-are-far-from-perfect-135799

[9] https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/

main parts: 1) a free text entry for the situation report, 2) a page of detail questions regarding the online meeting, and 3) demographic questions. For the detailed list of questions, refer to Appendix A.

*1.)* *Situation Description.* Firstly, we introduced participants to the general context of our research, i.e. the increased use of online meetings during lockdown for various purposes, including not only work but also leisure activities. We explained that we are interested in situations in which participants a) (unintentionally) provided insights into their own or b) learned something about another person’s private life. We asked them to describe the situation as accurately as possible. We also asked participants for the main protagonist in their report, i.e. whether the described situation revealed insights into their own or another person’s private life.

*2.)* *Details on Described Situation.* Secondly, we asked for details on the situation, taking into consideration who was the main protagonist, i.e., the participants themselves or somebody else, including the following:
- *Privacy Measures.* For self-reports, we asked for privacy measures that participants may have taken and their effect.
- *Story Source.* For reports about others, we asked for the source (e.g., participants of the same online meeting).
- *Bystanders.* We asked for other people being *physically* present and the relation between them and the protagonist (e.g., children, spouse, colleague).
- *Meeting meta-data.* We asked for details about the meeting, including the number of participants, purpose, time of day, the protagonists’ physical location, and whether this took place online before.
- *Predictability & Privacy Intrusion.* We put 7-point Likert items on whether participants considered the situation predictable, revealing information that would have kept secret otherwise, and violating the protagonist’s privacy.
- *Avoidance.* Lastly, we asked what could have been done to avoid the described situation.

*3.)* *Demographics.* Thirdly, we inquired participants’ demographic data including prior experience with video conferencing tools and working from home, as well as participants’ use of video conferencing software and their home office setup, to see whether this had an impact on described experiences. Lastly, we applied the IUIPC scale [21] to capture participants’ general privacy perception.

We provided options where appropriate, but most of the questions were to answer by free text entry. Personal questions, such as demographics and participants’ home office setup, were non-obligatory.

## 3.2 Recruitment

We recruited $N = 150$ participants via Prolific[10] and a total of $N = 50$ participants via university mailing lists and social networks. Completing the survey took approximately 15 minutes. Participants recruited via Prolific were compensated with 2£. Participants who completed the survey outside Prolific could (voluntarily) take part in a lottery of three Amazon vouchers with a value of 20€ each. We intentionally did not mention “privacy” in the invitation, nor on the first page of the survey to avoid bias.

## 3.3 Ethical Considerations

With the survey, we made sure to comply with all guidelines given by our institutions and the national data protection regulations to preserve participants’ privacy. We gathered participants’ consent on the first page of the survey, prior to data collection, and participants had to confirm that they are at least 18 years old. Questions concerning users’ personal home office settings as well as demographic data were non-obligatory. All data was stored anonymously on university servers. Finally, we did not connect participants’ e-mail addresses to the rest of the survey and deleted them after the raffle. Participation in the raffle was voluntary.

## 3.4 Limitations

Our sample is biased towards young female employees, hence our results may not apply to the general public. Furthermore, self-reports are a common tool to investigate users’ perception in security and privacy research [9, 28], but are prone to recall bias [26] or social desirability [35]. Also, privacy preferences are known to differ from users’ actual behavior (cf. the “privacy paradox” [14]), which may have impacted users’ reports on privacy measures. Finally, experimenter bias is a limitation of qualitative analyses and user reports might have been interpreted differently. However, we believe that this would not influence the resulting discussion.

## 3.5 Data Analysis

*Data Filtering.* To capture a broad set of experiences, we formulated an open prompt for participants to describe a situation related to online meetings during lockdown (cf. Appendix A). As a consequence, our dataset also included general descriptions of participants’ situations related to the pandemic, such as, e.g., activities that they could (not) do during the lockdown. As these were not meant to be the focus of this paper, we excluded such reports (a total of 57 reports, e.g., *“(...) I feel a lot more insecure and depressed. Not being able to meet friends and family, having to stay at home (...) made me sad and disappointed.”*, P455). Instead, we focused on reports that actually described a privacy intrusion (e.g., *“During quarantine, I joined some online fitness classes, where some people didn’t mute the mic and camera: I saw living rooms and people not involved walking by.”*, P586). Furthermore, we had to exclude three answers due to missing reports (2) and age reported under 18 (1). Hence, we ended up with a total of 140 answers (98 from Prolific) for our analysis, including 67 situations revealing information about the participants themselves (in the remainder of the paper referred to as *self-reports*) and 73 about somebody else (referred to as *outside-reports*).

*Thematic Analysis.* For the situation reports, we applied thematic analysis [3] as follows. First, two researchers independently went through a subset of reports (N=10 with 5 *self-reports* and *outside-reports* respectively) and applied open coding. In a review meeting, they discussed the codes and established an initial coding tree. Next, the researchers applied this coding tree to half of the dataset each (we made sure to split *self-reports* and *outside-reports* evenly across both halves). In a final review meeting, disagreements were resolved and the researchers agreed on the final set of codes. As we discussed disagreements and refined codes during the process,

[10] https://www.prolific.co/

**Table 1: Online Survey Results: Participants' age, gender, and employment status.**

| | | |
|---|---|---|
| *Age* | Min | 18 |
| | Max | 67 |
| | Mean | 29.46 |
| | Std | 9.58 |
| *Gender* | Female | 87 |
| | Male | 53 |
| *Employment Status* | employed full-time | 54 |
| | student | 51 |
| | employed part time | 17 |
| | self-employed | 9 |
| | Other | 5 |
| | unemployed and currently looking for work | 3 |
| | homemaker | 1 |

we do not report measures of interrater-agreement, following the recommendation by McDonald et al. [22].

*Recruitment Samples & Quotes.* To see whether our recruited sample groups might impact results, we compared the mean length of reports. We found only marginally differences in length (Prolific: 399.41, other channels: 410.57) and no differences while analyzing the reports. We translated quotes from the original language where necessary. We cite participants' ID as assigned by the survey tool.

# 4 RESULTS: USER STORIES OF PRIVACY AT HOME

We now present the results of our online survey and thematic analysis of situations (*self-reports* and *outside-reports*).

## 4.1 Participants

In this section, we describe our sample, including demographics, prior experience with home office and video conferencing, home office setups, online activities as well as general privacy perception.

*4.1.1 Demographics.* Of the 140 participants that we included in the analysis, 87 identified as female, and 53 as male. Participants' mean age was 29.46, and most (54) were employed full-time (refer to Table 1 for an overview).

*4.1.2 Experience with Home Office.* During the COVID-19 pandemic, most of our participants did work from home (Yes: 121, No: 11, Other: 8). Among the "other" answers, participants mentioned studying or taking classes from home (7), or having worked partly at home (i.e., only until June 2020, P539). Many of our participants (57) did never work from home before the pandemic, some occasionally (34) or rarely (29), and few often (14) or always (9).

*4.1.3 Experience with Video Conferencing.* The usage of online meeting software was popular among participants. In particular, only 4 participants stated to never use such software, while most used such software at least rarely (15), but rather occasionally (26), always (30), or often (64) (1 not answered).

*4.1.4 Home Office Setting.* Regarding their home office setup, many participants had an actual desk (51) and/or even a separate room (24) for their office setup, while others reported only using provisional setups, e.g. using a laptop on the sofa or in the kitchen. Some participants converted their spare rooms into offices (5), and some participants turned their dining table into a desk (6), e.g.:

> *"My temporary home office is my dining table. It is my only table surface that resembles a desk (...). The table is not used for dining as a result."*, P579

Few participants also mentioned a need to arrange with other household members working from home, e.g.:

> *"Study or living room, alternating with my partner"*, P231
> *"My 'Home Office' area is a small desk set up in a corner of our living room. We have a large living room, and my children have their home-schooling desk set-ups at the opposite end of the room. Other than our bedrooms, there is no other suitable spaces for these desks."*, P446

Some participants mentioned privacy considerations when describing their setup, e.g. *"back towards white wall, hence nothing can be seen in the background"* (P220) or a green wall that can easily be used for virtual backgrounds (P246). Note that this question was non-obligatory and three participants decided not to answer. Appendix B.1.1 provides a detailed overview.

*4.1.5 Online Activities.* Furthermore, many participants discovered new activities to be conducted at home using online meeting software (cf. Appendix B.1.2), including sports classes (30), dinners with friends (33), family meet-ups (56), or museum visits (9). Also other activities were mentioned such as online classes (8), meeting friends (7) to, e.g., watch movies (P288 and P548), analog games transferred to online meetups (4), virtual events (3) such as theater performances (P387) or movie festivals (P482), and online gaming (2). Two participants stated to have wished to try such activities but did not have the time to do so.

*4.1.6 Privacy Perception.* We assessed participants' general privacy perception using the IUIPC scale [21]. On a scale from 1 to 7, higher values indicate higher sensitivity towards privacy concerns. Participants rated their wish for *Control* (Min: 2, Max: 7, Mean: 5.94, SD: 1.07), their general privacy *Awareness* (Min: 2, Max: 7, Mean: 6.33, SD: 0.91) and data *Collection* in relation to personal benefits (Min: 1, Max: 7, Mean: 5.79, SD: 1.36). Table 2 in Appendix B provides detailed values per item.

## 4.2 Situations

From the reported situations, 73 were *outside-reports* (i.e., *"I learned something about another person's private life."*), and 67 were *self-reports* (i.e., *"I (unintentionally) provided insights in my own private life."*). For the *outside-reports*, participants mainly were in the same meeting (64) or the protagonist told them (8). One story source was stated as unknown. Reports were between 43 and 1920 characters long (Mean: 402.76, SD: 309.55). We now illustrate the results from our thematic analysis of reports (cf. Section 3.5 for the detailed procedure and Appendix B.2 for the full coding tree).

*4.2.1 Information Receivers.* Regardless of which perspective the situation was reported from, we found differences in *who* received the information about the main story protagonist. Among those, *peers* (e.g., fellow students or colleagues) were mentioned most (68):

> *"Student in my university was watching a zoom class while taking a shower. He accidentally left the camera on. Hilarity ensued."*, P505
> *"I learned which of my colleagues have children (...)"*, P180

Frequently, *superiors* (e.g., the protagonists' teacher or boss, 23) or *subordinates* (e.g., the protagonists' employees or students, 25) gained insights:

> *"With online meetings with teachers for classes, I have unintentionally shared aspects of my life that normally they would not know, such as my cats appearing on camera or my family members calling me. My bedroom is also something that I usually don't enjoy showing, and I had to. It is interesting because even though we are apart, we can see more private aspects of each other's lives."*, P517
> *"My boss heard my new partner (a former colleague) in the background (...) and thus learned about the relationship."*, P231
> *"My professor had a guitar in the background and then started to tell us that he likes to play guitar."*, P208

Other situations included *friends* (14):

> *"Last month I was having an online meeting with 4 friends that I met at university (...)"*, P476

*4.2.2 Information Channel.* Our situation reports also differed as to *how* the respective information was revealed. Most information was observed from the victim's *camera image* (74), but also *audio* (44) played an essential role at times:

> *"(...) It thus happened frequently that my cat sneaked into the camera image."*, P288
> *"As a student, I have multiple online classes in Zoom. In one of the classes, the teacher's dog starts barking and didn't shut up and then he shouted [at] the dog very aggressively and the class started to laugh."*, P472

Few reported on *shared desktop* (3) content and the *personal information* (3) necessary to run/join the meeting platform revealing information, e.g.:

> *"We had a lecture on the video platform zoom and the professor unintentionally shared [their] browser window where it was clearly visible that [the professor] was planning to go on vacation."*, P293
> *"We were asked several times to provide personal data such as address, name (...) to enable logging into online meeting platforms."*, P416

*4.2.3 Information.* The information that got revealed mainly concerned the protagonists' *living situation* (58) or *family relations* (51):

> *"During an online zoom meeting with a manager (...). As she moved rooms I had an insight into how large her property was."*, P398
> *"My younger brother came in to my bedroom/office while I was on an online meeting with colleagues and professors and he appeared on the camera so that everyone saw him."*, P498
> *"In an online meeting with a friend, I recognized a girl in the background – indicating that what was initially dismissed as a flirtation turned into something serious."*, P262

Further, the protagonists' *personal characteristics* (19), *hobbies* (10) or *pets* (14) were mentioned, e.g.:

> *"(...) While we were discussing the topic of our presentation one of my teammate's girlfriend showed up and told her that she had to leave because her shift at work was starting and they kissed in front of the camera: we discovered in this unusual way that she's a lesbian."*, P476

Other information included the protagonists' *(mental) health state* (5), current *location* (4), or handling of the *lockdown* situation (3), e.g.:

> *"One day I was in a Zoom meeting with some colleagues from work and we hear a bell ringing. It was my colleague's phone. She excuse herself from the meeting to attend the phone and we started hearing screaming and crying. She then came and excused herself from the meeting and [left] abruptly. Some days passed and we then got back from her. She was devastated and informed us that a brother of hers was diagnosed with COVID-19 (...)"*, P548
> *"It was possible to learn where everyone's parents' home is, since during the pandemic many students traveled back. (...) Also, camera streams often show one's parents in the background. (...)"*, P214
> *"I learned a lot about how my friends handle being away from other people and saw the differences in how they each handle it differently."*, P423

Also intimate insights were mentioned:

> *"Somebody accidentally turned on the camera (...) and was naked (...)"*, P234

*4.2.4 Intention.* Though we were asking participants for privacy insights that were *unintentionally* (25) revealed (e.g., *"(...) I (...) didn't notice that the mute function was deactivated (...)"*, P265) some also reported on *actively* (26) having shared private information during online meetings:

> *"During some zoom meetings I was able to talk with my colleagues in a more personal way. So, we all talked about the changes in our lives. One of my teammates told me she was facing some bad times with her daughter as she was at home, without school or extra activities (...). She was really down and we shared some insights. (...)"*, P484

Few also mentioned that information reveal was *involuntary* (4), e.g.:

> *"I had an important meeting at work while we were still quarantined. Everyone could see the inside of my house and I was not comfortable with that, but had no other choice. (...)"*, P452

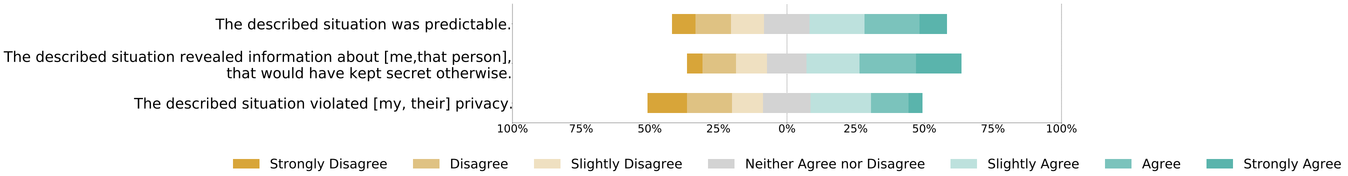

**Figure 1: Online Survey Results: Participants assessed whether the described situation was predictable and privacy-invasive on 7-point Likert scales.**

*4.2.5 Miscellaneous.* We found a few other themes in the situation reports. Some participants included their feelings towards the whole situation and reported on their *personal* (8) or *positive* (3) experience, while others felt *uncomfortable* (2). Others (3) also mentioned that knowing new details about each other created a *friendly* atmosphere, made them feel closer, and increased trust, e.g.:

> *"(...) To summarize, I have never learned so much about the private life of a lecturer (...). First, this was a bit strange, but it became less after a certain familiarity developed. (...)"*, P304

## 4.3 Online Meeting Details

We asked participants for a number of details regarding the online meeting in which the privacy intrusion happened (cf. Appendix A.2 for full list of detail questions). In particular, most meetings (80) were conducted for business purposes, and 15 private. Other purposes were mentioned, e.g. university (20) or school/classes (13) (1 participant preferred not to answer). Most of these did never take place online before the pandemic (85).

Meetings were of varying sizes with up to 250 participants (Mean=19.21, SD=38.04, 15 unknown). Most meetings took place in the afternoon (45) or in the morning (39). In 71 reports other people were physically present (i.e., with the main protagonist) during the meeting (no other people in 69 reports). Those people were mainly the protagonists' partner (22), child(ren) (17) or colleague(s) (17). Most participants reported the person in question was in their living room (40), bedroom (20), or study (17) during the described situation.

Participants were rather neutral whether or not the described situation was predictable (Median=4.5 on a 7-point Likert scale) or violated the protagonist's privacy (Median=4), but slightly agreed that the revealed information would have stayed secret otherwise (Median=5, cf. Figure 1).

## 4.4 Privacy Measures and Effect

For the *self-reports*, all (67) participants mentioned at least one measure they had taken to protect their privacy. Among those, controlling the background (29) was the most popular: either using a neutral, real one, applying a virtual background, or using blur:

> *"Prevent one from perceiving exactly the context in which I am"*, P418
> *"Moved to an area of my home which has a plain background (No photos, mess in the background etc)"*, P440

However, P410 indicated to use virtual backgrounds for fun rather than for privacy protection. Another popular measure was to tidy up the space (21) or turn the camera off (19).

> *"I cleaned up the space behind me and removed things that I didn't want to share with the rest of the group, e.g. photos of me and my partner, medications etc"*, P575
> *"I bought a laptop without camera, so I can have the camera on only when I wanted it to be."*, P471

Others (e.g., P513) would still turn the camera on in case it was necessary for a class.

In summary, participants mentioned between 0 and 5 measures (Mean=1.95, SD=1.13) that they took to protect their privacy. We also asked whether participants considered these measures to be effective. Most participants stated that their efforts were successful (47), apart from some that did not or only partly work as expected (4 each), e.g. due to the meeting being too spontaneous (P538), or a remaining discomfort:

> *"Yes as it meant the people on the call could only see what I allowed them to see, although I still felt as though I had lost some privacy as this is not usually an area of my life many people would get to see."*, P575

Few described measures as too late (2) or not applicable (2).

## 4.5 Avoidance

We also asked participants what could have been done to *avoid* the described situation (5 did not answer). Some stated that nothing (15) could have been done or that avoidance was not necessary (9). Among concrete measures, turning off (11) or covering (2) the camera were most popular. Also using another background – be it real, but neutral (7) or virtual (5) – was suggested. Others would lock the door/room (12) or arrange with other people (11) being involved physically (e.g., *"I could have set up strict rules with my husband about what to do and not do during working hours."*, P482). Participants also suggested to disclosing less (personal) information (9) when talking in online meetings. The most drastic suggestion was to not join the meeting in the first place (9). However, many participants stated that the suggested measures are not ideal as, e.g., they would risk losing the internet signal when moving to another room (P557) or even lose their job (P550), they could not lock out their children (P304) or P558 who stated: *"I could have decided not to take dance classes online (...) but this was not an option (...)"*

## 4.6 Summary

Our survey showed that privacy-relevant information (e.g., living situations or family relations) got revealed during online meetings.

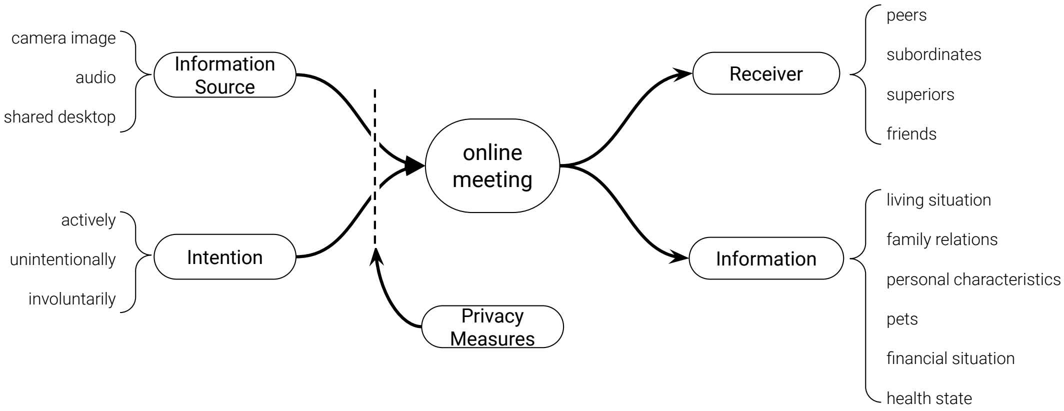

**Figure 2: Privacy Intrusion in Online Meetings: Our analysis revealed a number of information sources, receivers, and types of information. Users' intentions also influence the potential information reveal. Privacy measures can help preventing this.**

Being actively, unintentionally, or involuntarily revealed via camera, audio, or shared desktop content, this information reached various stakeholders (e.g., peers, superiors, or subordinates). Privacy measures can help users prevent such information from being shared (refer to Figure 2 for an overview). However, measures suggested by our participants only had limited effect, as we still found them unintentionally sharing personal information and/or feeling uncomfortable. As such, we discuss potential means to support users in protecting their and others' privacy during online meetings in the next section.

## 5 DISCUSSION & FUTURE RESEARCH DIRECTIONS

Our results show that online meetings pose a risk to users' privacy, as they provide audio- and video-based insights into their private spaces. Personal information that would have stayed secret otherwise might be revealed. This might include intimate insights such as nudity (P234) or family and intimate relationships (e.g., P262).

In our survey, most information was revealed via the camera image or audio stream. While turning off both or not joining the meeting at all is a drastic but effective measure, it is often not desirable. As an example, P558 could not go through lockdown without their dance classes. Also, presentations can be more effective if presenters actually see the audience [24]. Hence, we suggest supporting online meeting participants to protect their privacy, while allowing them to be active members of the meeting (e.g., using camera/audio as desired). We now discuss concepts that could empower users *before*, *during*, and *after* the meeting to protect their privacy.

### 5.1 Before the Meeting: Awareness & Setup

Related work highlighted privacy concerns with regard to data collected by devices within the home [1, 33, 39]. At the same time, users generally wish to be aware of their personal data being captured, stored, and/or shared [11, 15, 23]. Means to address this are privacy labels on devices' packaging [10, 12, 17], QR-Code stickers carrying further information about devices' data policies [40], privacy visualizations [29], or device locators [32]. These, however, are not quite applicable to the scenario of online meetings: the devices' (i.e., laptops', PCs', or cameras') packaging might not be in users' hands anymore; QR-code stickers or other information would need to be provided to all meeting participants as well as to potential (physical) bystanders; device locators would need to be spread across all participants' setups.

Moreover, users tend to skip and agree to privacy policies [36]. This issue has been acknowledged in research: prior work investigated, e.g., the design of privacy notices and UIs [19, 31] or personalized privacy assistance [6]. However, these usually only concern the installation procedure and/or configuration of devices or software.

We argue that for online meetings, it is not only the software, nor the devices that pose a challenge to users' privacy. Our online survey showed that privacy breaches happened within the meeting itself, via, e.g., the audio or video stream. Also personal data that was necessary to access a certain platform was mentioned. Both were unexpected and uncomfortable to users. To address this, future work should investigate how to a) increase awareness for privacy in video-based online meetings in general and b) support the setup and c) joining on a per-meeting basis.

*Awareness.* To increase users' awareness, a common measure is to clearly indicate that data is being recorded. For instance, most webcams provide an LED light to indicate that they are on (i.e., recording video) – however, these are frequently overlooked by users [5, 27]. Prior work suggested *tangible privacy indicators* to address this. Examples of such tangible privacy indicators include the *EyeCam* [34], a webcam that resembles a human eye or the *Status Flower* [20], a flower-shaped prototype, which closes its petals to cover the camera.

However, for the online meeting scenario, it might not only be relevant *that* but also *what* is being recorded, e.g. if users' surroundings or bystanders are on camera as well. This might not be apparent once in the meeting, in particular when users cannot see their own camera view (for example, while giving a presentation). Related work suggested providing feedback on how much privacy is currently maintained [25]. In contrast, an indicator could also inform users about the current level of privacy intrusion. Measures to inform such an indicator could be, e.g., how much content apart from the speaker is currently visible to other meeting participants.

Furthermore, many online meetings are held for business purposes (more than half in our online survey), as users were working from home, especially during the pandemic. In such cases, not only the personal, but also the company's privacy is at risk. Hence, it is also the employers' responsibility to generate awareness for potential privacy risks [16].

*Setup.* Another approach could be to help users already before joining the meeting when preparing their setup at home. A visualization tool (e.g., based on augmented reality) could highlight areas that are being covered by the webcam [29]. With such a tool, users could inspect their surroundings prior to the meeting and actively choose what will be visible during the meeting. This would help users to, e.g., search for another space with a more neutral background and/or remove personal items that they do not want to be shown. Many participants also stated a need to arrange with other household members when setting up for their meetings. P288 suggested a physical door sign to prevent others from entering the room. Many participants would also lock the room completely. Another option could be to send notifications to other household members' personal devices, inform them about the meeting and, hence, prevent interruptions later during the meeting.

*Joining the Meeting.* Many platforms require users to share personal data (e.g., names) to use it, which was uncomfortable for our survey participants. Related work suggested the use of pseudonyms [16]. A privacy mechanism could support users to choose and/or automatically generate such pseudonyms. Furthermore, a privacy label [10, 12, 17] could be shown before joining the meeting to indicate, e.g., whether or not this meeting will be recorded and where the recording will be stored. Also, some communication tools allow checking the own camera image before actually joining the meeting (e.g., Zoom). To support users' privacy, this camera image could be augmented to highlight areas that are being shown and inform users about which privacy-relevant information might be contained (e.g., photos on the wall might hint at favorite activities or places). As a consequence, users could decide to move to another place or turn the video off completely.

## 5.2 During the Meeting: Preserving Privacy

Though being aware and having taken adequate measures prior to the meeting, users might still be victims to – potentially unpredictable – privacy-intrusive events during the meeting.

To address this, easy methods to (spontaneously) block recording should be employed [25]. Examples are gestures to cover the camera or mute the microphone. Microphones could also follow a general "push to talk" mechanism[11], i.e. users would need to actively agree to their audio being recorded. As such, the accidental transmission of audio (e.g., P265 did not notice the mute function being deactivated) would be prevented. At the same time, this supports the "privacy by default" approach which is now established in many national data protection regulations. Another option is to mute the microphone automatically if voices other than the speaker (e.g., other household members) are recognized.

Another aspect in our survey results was information disclosure during talking in online meetings, i.e. by the participants themselves. We assume that their home environment, considered safe and private, might have led participants to reveal more private information. To counteract this, a warning message during the meeting could remind users of the context they are in (e.g., a business meeting), other meeting participants and their roles (e.g., their boss or supervisor), and of their data potentially being recorded and shared.

As for the camera image, users could employ measures to disrupt face recognition (e.g., wearing a mask) [16], which however might not be desirable in serious contexts. Moreover, many participants and related work [16] suggested using a generic/neutral background like, e.g., a white wall. In cases this is not possible, filters can be applied to, e.g., blur the background. For presentations being held in online meetings, another option is to spotlight single audience members to the presenter only [24] instead of audience members being visible to all other meeting participants.

However, while these measures protect users' privacy, they do not protect others who might enter the recording space unknowingly (e.g., spouses, children, roommates). Detecting others walking into the room [25] or moving parts in the image apart from the speaker could serve as a basis for this. Recognizing potential observers/bystanders has been previously applied for security purposes [30], but could be further explored for online meetings. A potential mechanism could indicate who is potentially seen in the online meeting and/or deliver warnings to users as well as bystanders. Another option is to blur parts of the image or turn the video stream temporarily off once background activity has been detected. Lastly, other meeting participants' attention could hint at privacy-relevant content being revealed. As an example, by means of eye tracking, it could automatically be detected whether the speaker or their background is currently at the focus of attention.

## 5.3 After the Meeting: Retrospective

Some meetings are being recorded and published afterwards. As an example, many conferences held live sessions that are available online ever since[12]. As a consequence, it can be completely unknown and unpredictable to users who will finally see their performance. Related work showed that meeting recordings or related social media postings can reveal privacy-relevant information and suggested limiting recording and sharing [16]. However, in many cases, a recording is valuable to reach a broader audience. If a recording is started within the meeting, online meeting software such as Zoom usually raises a voice pop-up to inform participants with the option to quit. Furthermore, meeting hosts are obliged to inform participants about the recording prior to the meeting. A potential additional measure could be to provide participants with (parts of) the recording to gather additional consent for it being published or otherwise provide the option to revoke consent. This is especially useful in cases where, e.g., children or partners unexpectedly appeared in the video stream. Such incidents might change users' minds in a way that they do not want this to be published and/or shared. Another option is to filter privacy-sensitive content from recordings automatically by, e.g., applying motion

[11] e.g., in Zoom https://support.zoom.us/hc/en-us/articles/360000510003-Push-to-talk

[12] e.g., IEEE S&P 2020 Opening, https://youtu.be/K5MNe8bwLMk

detection/tracking algorithms to identify dynamic content in the image that is not the speaker.

## 6 CONCLUSION

In this paper, we present results from our online survey in which we collected users' experiences with potential privacy intrusion in online meetings. We found that camera and audio streams frequently revealed insights into meeting participants' private lives, including their living situation or familiar relations. We suggest on one hand increasing users' privacy awareness towards not only video conferencing software but also online meetings themselves. On the other hand, potential measures to support users in protecting their privacy could be applied before, during, and after an online meeting. Our work is useful for future researchers and practitioners to support meeting hosts and participants of online meetings in protecting their privacy.

## ACKNOWLEDGMENTS

We would like to thank all survey participants for sharing their experiences with video-based online meetings during the pandemic. This project has received funding from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), Grant No. 425869382, and is part of the Priority Program SPP2199 Scalable Interaction Paradigms for Pervasive Computing Environments.

## REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '19)*. USENIX Association, Berkeley, CA, USA, 1–16.

[2] Tabrez Ahmad. 2020. Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. https://doi.org/10.2139/ssrn.3568830

[3] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. (2012).

[4] Aaron R. Brough and Kelly D. Martin. 2021. Consumer Privacy During (and After) the COVID-19 Pandemic. *Journal of Public Policy & Marketing* 40, 1 (2021), 108–110. https://doi.org/10.1177/0743915620929999 arXiv:https://doi.org/10.1177/0743915620929999

[5] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. 2015. HCI in Business: A Collaboration with Academia in IoT Privacy. In *HCI in Business*, Fiona Fui-Hoon Nah and Chuan-Hoo Tan (Eds.). Springer International Publishing, Cham, 679–687.

[6] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[7] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[8] Carole Després. 1991. The Meaning of Home: Literature Review and Directions for Future Research and Theoretical Development. *Journal of Architectural and Planning Research* 8, 2 (1991), 96–115. http://www.jstor.org/stable/43029026

[9] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4254–4265. https://doi.org/10.1145/3025453.3025636

[10] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, USA). IEEE, New York, NY, USA, 447–464. https://doi.org/10.1109/SP40000.2020.00043

[11] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[12] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 534, 12 pages. https://doi.org/10.1145/3290605.3300764

[13] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. 2020. The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20)*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3419394.3423658

[14] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002

[15] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799

[16] Dima Kagan, Galit Fuhrmann Alpert, and Michael Fire. 2020. Zooming Into Video Conferencing Privacy and Security Threats. arXiv:2007.01059 [cs.CR] https://arxiv.org/pdf/2007.01059.pdf

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

[18] Navid Ali Khan, Sarfraz Nawaz Brohi, and Noor Zaman. 2020. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. https://doi.org/10.36227/techrxiv.12278792.v1

[19] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[20] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-Worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction* (Stockholm, Sweden) *(TEI '18)*. Association for Computing Machinery, New York, NY, USA, 177–187. https://doi.org/10.1145/3173225.3173234

[21] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[22] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages. https://doi.org/10.1145/3359174

[23] Mateusz Mikusz, Steven Houben, Nigel Davies, Klaus Moessner, and Marc Langheinrich. 2018. Raising Awareness of IoT Sensor Deployments. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*. IET, London, UK, 8 pages. https://doi.org/10.1049/cp.2018.0009

[24] Prasanth Murali, Javier Hernandez, Daniel McDuff, Kael Rowan, Jina Suh, and Mary Czerwinski. 2021. AffectiveSpotlight: Facilitating the Communication of Affective Responses from Audience Members during Online Presentations. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 247, 13 pages. https://doi.org/10.1145/3411764.3445235

[25] Carman Neustaedter, Saul Greenberg, and Michael Boyle. 2006. Blur Filtration Fails to Preserve Privacy for Home-Based Video Conferencing. *ACM Trans. Comput.-Hum. Interact.* 13, 1 (March 2006), 1–36. https://doi.org/10.1145/1143518.1143519

[26] Delroy L Paulhus, Simine Vazire, et al. 2007. The self-report method. *Handbook of research methods in personality psychology* 1, 2007 (2007), 224–239.

[27] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. 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* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1649–1658. https://doi.org/10.1145/2702123.2702164

[28] Sarah Prange, Lukas Mecke, Michael Stadler, Maximilian Balluff, Mohamed Khamis, and Florian Alt. 2019. Securing Personal Items in Public Space: Stories of Attacks and Threats. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (Pisa, Italy) *(MUM '19)*. Association for Computing Machinery, New York, NY, USA, Article 27, 8 pages. https://doi.org/10.1145/3365610.3365628

[29] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView – Exploring Visualisations Supporting Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3313831.3376840 in print.

[30] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 147–152. https://doi.org/10.1145/3282894.3282919

[31] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[32] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[33] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Berkeley, CA, USA, 16 pages.

[34] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing Relations between Humans and Sensing Devices through an Anthropomorphic Webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 622, 13 pages. https://doi.org/10.1145/3411764.3445491

[35] Roger Tourangeau and Ting Yan. 2007. Sensitive questions in surveys. *Psychological bulletin* 133, 5 (2007), 859.

[36] T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. 2016. Make It Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5252–5256. https://doi.org/10.1145/2858036.2858149

[37] M. Weiser, R. Gold, and J. S. Brown. 1999. The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal* 38, 4 (1999), 693–696.

[38] Paweł W. Woźniak, Thomas Kosch, Eleonora Mencarini, Andrzej Romanowski, and Jasmin Niess. 2021. 'I Would Have Preferred an Ankle Tag': The Lived Experience of a Nationwide Quarantine App. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction* (Toulouse & Virtual, France) *(MobileHCI '21)*. Association for Computing Machinery, New York, NY, USA, Article 43, 13 pages. https://doi.org/10.1145/3447526.3472063

[39] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[40] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[41] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 65–80.

[42] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200. https://doi.org/10.1145/3274469

[43] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216. https://doi.org/10.1515/icom-2019-0015

# A ONLINE SURVEY

## A.1 Part 1: Situation

In the following, we will ask you to describe a situation that you have recently experienced in connection with measures taken in the context of the Corona pandemic. In particular, we are interested in a situation, in which you

- (unintentionally) provided insights in your own private life or
- learned something about another person's private life.

Especially consider online meetings, that were increasingly used during "home office" or to keep up leisure activities during lockdown and quarantine (e.g. participation in online sports courses via online meetings). Furthermore, we will ask you about additional details on the situation and on your experience with such online meetings.

- Please describe the situation as accurately as possible. [free text entry]
- Who is the main protagonist in this situation?
  - **myself**
    I (unintentionally) provided insights in my own private life.
  - **somebody else**
    I learned something about another person's private life.

## A.2 Part 2: Details

Depending on the participants' choice of [myself, somebody else] (see above), we adapted the following detail questions:

- Which measures did take to protect privacy during these activities? (e.g., use virtual backgrounds, turn off webcam, clean up your apartment, etc. ...)
  *<free text entry>* [for **myself**-situations only]
- Please describe if and how your applied measures had the intended effect.
  *<free text entry>* [for **myself**-situations only]

---

- How did you know about this story?
  (e.g., I was a participant in the same online meeting; that person told me; ...)
  *<free text entry>* [for **somebody else**-situations only]

---

- Was anbody, apart from [yourself, this person], physically present in this situation?
  Yes, *<number>* other people. | Nobody else was present.
- How is the relation between [yourself, this person] and these other people? (e.g., children, spouse, colleague)
  *<free text entry>*
- How many participants attended the online meeting? Please add the (rough) number of participants, including yourself, if need be.
  *<number>* | I don't know.
- What was the reason for the meeting?
  business | private | other (please specify)
  | Prefer not to say
- Did this activity take place online before?
  Always | Often | Occasionally | Rarely | Never
  | Prefer not to say

- At what time of day did the described situation occur?
  in the morning | forenoon / noon | in the afternoon | in the evening | at night | Other (please specify)
  | I don’t know
- Where [were you, was that person] during the online meeting? (e.g., in the kitchen, in the office, on the go, ...)
  *<free text entry>*
- The described situation was predictable.
  *<7-point Likert scale>*
- The described situation revealed information about [me, that person], that would have kept secret otherwise.
  *<7-point Likert scale>*
- The described situation violated [my, their] privacy.
  *<7-point Likert scale>*
- Please describe what [you, this person] could have done to avoid the described situation.
  *<free text entry>*

## A.3 Part 3: Demographics

- With which gender do you identify most?
  female | male | other | prefer not to say
- How old are you?
  I am *<number>* years old.
- What describes your current employment status best?
  - employed full-time
  - employed part time
  - unemployed and currently looking for work
  - unemployed and not currently looking for work
  - student
  - retired
  - homemaker
  - self-employed
  - unable to work
  - Other
  - Prefer not to say
- Did you work from home during the COVID-19 pandemic?
  Yes | No | Other | Prefer not to say
- Did you work from home before?
  Always | Often | Occasionally | Rarely | Never | Prefer not to say
- Please describe where and how you set up your “home office”.
  *<free text entry>*
- How often are you using online meeting software? (e.g., Skype, Zoom, Jitsi, Webex, ...)
  Always | Often | Occasionally | Rarely | Never | Prefer not to say
- Which activities did you start doing at home? Please choose all that apply.
  - Participation in online sports classes
  - Virtual dinner with friends
  - Virtual family meet-ups
  - Virtual museum visits
  - Other (please specify)
  - None of these
- 10-item IUIPC scale [21]

# B ONLINE SURVEY RESULTS

## B.1 Participants

*B.1.1 Home Office Setups.* Participants’ description of their home office setup by room/place, desk, and device.

| | | |
|---|---|---|
| *room/place* | living room | 28 |
| | bedroom | 27 |
| | separate room | 17 |
| | own room | 14 |
| | kitchen | 6 |
| | spare room | 5 |
| | dining room | 5 |
| | office | 4 |
| | couch | 3 |
| | own room in parents’ house | 3 |
| | desk | 3 |
| | bed | 3 |
| | sleeping couch | 2 |
| | student apartment | 2 |
| | no home office | 2 |
| | other | 12 |
| *desk* | desk | 51 |
| | dining table | 6 |
| | table | 6 |
| | coffee table | 1 |
| | folding table | 1 |
| | market table | 1 |
| | PC | 1 |
| | provisional desk | 1 |
| | living room | 1 |
| *device* | laptop | 37 |
| | external monitor | 16 |
| | PC | 12 |
| | computer | 9 |
| | notebook | 4 |
| | headphones | 4 |
| | company’s laptop | 4 |
| | office supplies | 3 |
| | mouse | 2 |
| | headset | 2 |
| | paperwork | 2 |
| | books | 2 |
| | webcam | 2 |
| | other | 18 |

*B.1.2 Online Activities.*

- Participation in online sports classes (30)
- Virtual dinner with friends (33)
- Virtual family meet-ups (56)
- Virtual museum visits (9)
- Other (28)
  - lessons/classes (8)
  - friends (7)
  - analog game (4)
  - virtual events (3)
  - quiz (2)
  - no time (2)
  - online gaming (2)
  - messaging (1)
  - shopping (1)
  - business meetings (1)
- None of these (41)

#### *B.1.3 IUIPC.* Detailed results for the IUIPC scale [21].

**Table 2: Participants' ratings per IUIPC item in the respective categories Control, Awareness and Collection [21].**

| | | min | max | mean | SD |
|---|---|---|---|---|---|
| *Control* | Consumer online privacy is the consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. | 3 | 7 | 5.95 | 1.05 |
| | Consumer control of personal information lies at the heart of consumer privacy. | 2 | 7 | 5.91 | 1.14 |
| | I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. | 2 | 7 | 5.96 | 1.02 |
| *Awareness* | Companies seeking information online should disclose the way the data are collected, processed, and used. | 3 | 7 | 6.46 | 0.86 |
| | A good consumer online privacy policy should have a clear and conspicuous disclosure. | 4 | 7 | 6.46 | 0.77 |
| | It is very important to me that I am aware and knowledgeable about how my personal information will be used. | 2 | 7 | 6.06 | 1.03 |
| *Collection* | It usually bothers me when online companies ask me for personal information. | 2 | 7 | 5.6 | 1.39 |
| | When online companies ask me for personal information, I sometimes think twice before providing it. | 1 | 7 | 5.93 | 1.24 |
| | It bothers me to give personal information to so many online companies. | 1 | 7 | 5.81 | 1.40 |
| | I'm concerned that online companies are collecting too much personal information about me. | 1 | 7 | 5.68 | 1.39 |

## B.2 Coding Tree for Situation Reports

- situation protagonist
  - myself (67)
  - somebody else (73)
- Information Receivers
  - peers (68)
  - friends (14)
  - superior (23)
  - subordinate (25)
  - other
    - not specified (15)
    - client (2)
    - landlord's daughter (1)
    - sister's friends (1)
    - childcare person (1)
    - politics (1)
    - clients (1)
    - parliament (1)
- Information Channels
  - shared desktop (3)
  - camera image (74)
  - microphone/audio (44)
  - other
    - not specified (6)
    - personal information (3)
    - virtual backgrounds (1)
    - online/social media (1)
    - in presence (1)
    - images in background (1)
    - in person (delivering) (1)
- Information
  - financial situation
  - living situation
  - family relations
  - bystanders
  - personal characteristics
  - hobbies
  - pets
  - other
    - (mental) health state (5)
    - location (4)
    - not specified (4)
    - handling lockdown situation (3)
    - private life / information (3)
    - name (2)
    - other/miscellaneous (16)
- Intention
  - intentionally (26)
  - unintentionally (25)
  - involuntarily (4)
- Miscellaneous
  - personal experience (8)
  - positive experience (3)
  - (generic) privacy intrusion (8)
  - new people (4)
  - uncomfortable (2)
  - friendly/human (3)