Understanding User Privacy Perceptions in Video Conferencing: Insights from a Feature-Specific User Study

Hobin Kim
KAIST
ghqls1237@kaist.ac.kr

Wonho Song
KAIST
swh0329@kaist.ac.kr

Joseph Seering
KAIST
seering@kaist.ac.kr

Min Suk Kang*
KAIST
minsukk@kaist.ac.kr

Abstract

The widespread adoption of video conferencing platforms has raised privacy concerns. Recent studies have shown that users express various concerns, such as reluctance toward mandatory camera-on policies, but these findings remain coarse-grained, lacking details on specific features and social relationships. This paper investigates how users perceive privacy with respect to various features in video conferencing platforms. Using the framework of contextual integrity, we analyze information flows across diverse scenarios, such as business meetings and online classes. Our findings reveal nuanced privacy perceptions regarding features that have been discontinued (e.g., attention tracking) or adjusted (e.g., meeting recording), suggesting that the handling of these features could have aligned better with users' privacy expectations. Additionally, we identify emerging privacy concerns about the pinning and spotlighting features, as users often feel great discomfort when their video is pinned or spotlighted by others in specific contexts. These insights provide a deeper understanding of privacy in video conferencing, highlighting the need for more refined privacy controls and a proactive approach to feature development.

Keywords

Privacy, video conferencing, contextual integrity

1 Introduction

Since the advent of COVID-19, the use of video conferencing for business meetings, classes, and conferences has increased significantly [49]. While video conferencing platforms have become an essential tool, they may at times expose personal aspects of our lives to other participants including details from our private spaces. This unintended exposure has raised significant privacy concerns among users. To understand these concerns, prior research has investigated various aspects of privacy in video conferencing. For example, studies have examined users' privacy concerns in diverse contexts [17], privacy-invasive incidents experienced during video calls [30], and shifts in user perceptions toward video conferencing during and after the pandemic [57]. These provide valuable insights into general privacy concerns, but fall short of fully describing users' perspectives regarding the interplay between features and usage contexts in video conferencing.

Specific features in video conferencing platforms often introduce unique privacy concerns that may not be properly captured by general privacy studies. One example is Zoom's attention tracking feature, which allowed hosts to monitor participant engagement in real time during a conference call (by monitoring whether Zoom is the active window of each participant). Due to significant privacy concerns raised by users, Zoom removed this feature in April 2020 [50]. This incident highlights the tension (see a heated online debate [37, 39]) between platform capabilities and user privacy expectations. Another example is Zoom's recording feature, which initially did not consistently notify participants when recording commenced. In response to privacy concerns (e.g., potential unauthorized recording), however, Zoom introduced a consistent notification system in May 2021, including an audio announcement to ensure that participants were aware of the recording [41]. More recently, Microsoft Teams has adopted a similar, more privacy conscious approach by adding consent for meeting recording in March 2023 [45]. These examples show how our limited understanding of user privacy in the context of video conferencing features leads to reactive changes, addressing problems only after controversies emerge.

In this paper, we explore users' privacy concerns regarding specific features and assess whether these features align with users' privacy expectations. We employ an online survey with 769 users of video conferencing tools to gain insights about users' privacy concerns toward different features under various social contexts in video conferencing platforms. We define privacy in video conferencing as the right of individuals to control the amount of information shared about themselves with other participants during a session. Though there are also important privacy issues regarding private information shared with the platform, in this paper we focus on privacy issues emerging from interactions between users.

We focus on a small set of features that have potential privacy implications in multi-participant video conferencing sessions. After a criteria-based selection process, we chose four features: *attention tracking* (a feature that allows hosts to monitor participant attentiveness during a meeting), *meeting recording* (a feature that allows hosts to video record meetings), *pinning* (a feature that allows any participant to enlarge another participant's video feed), and *spotlighting* (a feature that allows hosts to enlarge a participant's video

*Corresponding author.

Proceedings on Privacy Enhancing Technologies YYYY(X), 1–29

https://doi.org/XXXXXXX.XXXXXXX

feed to everyone's screen); see Section 3.1 for more detailed description and the selection process. As we study these features, we group them into three categories: features that have been *removed* due to privacy concerns (e.g., attention tracking), features that have been *updated* in response to privacy concerns (e.g., meeting recording), and features that have *not yet* been the focus of significant privacy discussions (e.g., pinning and spotlighting); see Section 3.1 for details.

To investigate users' privacy perception towards selected features, we apply the framework of privacy as *contextual integrity* [28], which maintains that privacy is preserved when information flows align with the contextual norms of the user population under study. Video conferencing features often introduce new information flows between participants; e.g., a high-quality video feed is sent to one or more other participants when being pinned or spotlighted. Contextual integrity allows us to assess how users perceive these information flows in various contexts (e.g., business meetings, online lectures, and social gatherings). Beyond analyzing the flow of information, we also explore how users' privacy perceptions shift depending on the role of the participants in these contexts. We also investigate how user privacy perceptions are influenced by different conditions or transmission principles, such as when explicit consent is obtained or when participants are given control over how much information they share. Additionally, we examine how gender and prior experience with the features we test impact privacy perceptions.

In this paper, we address the following research questions:

(RQ1) *What privacy concerns do users have about features that have been removed? How serious are these concerns?*
Insights: Users have noticeable privacy concerns about the discontinued attention tracking feature, hence justifying its removal. However, explicit consent, notifications during use, and anonymization of attention data could very well alleviate these concerns, suggesting that the feature could have been enhanced with privacy-conscious updates rather than removed entirely.

(RQ2) *What privacy concerns do users have about features that have been updated in response to previous privacy issues? Are they satisfied with the changes?*
Insights: The update requiring consent for meeting recordings is positively received, but privacy concerns remain about unclear data retention and access policies. Clearer guidelines on these issues could further improve user privacy.

(RQ3) *Can potential privacy concerns be identified in features that video conferencing platforms have not yet regarded as risks (though some users have expressed concerns about them)? How do these concerns compare to those of features that have been removed or updated?*
Insights: Users have significant privacy concerns about the pinning and spotlighting features. Consent, notifications, and user control over pinned video size/duration could address discomfort significantly, especially when pinned by strangers. Spotlighting is generally more accepted but raises issues when participants are spotlighted while muted.

Our study aims to introduce context-dependent subtleties into the ways we think about privacy in video conferencing. By applying the theory of privacy as contextual integrity, we have identified previously unexplored privacy concerns in video conferencing features. This approach provides a solid basis for designing features that better align with users' expectations and privacy needs compared to existing feature designs.

2 Background and Related Work

The widespread adoption of video conferencing has exposed users to privacy risks such as unauthorized meeting access [24], undisclosed data mining [22], and accidental exposure of sensitive information [2]. These challenges have spurred research into users' privacy perceptions and the broader implications of video conferencing technology. This section reviews studies on privacy concerns in video conferencing (Section 2.1), explores privacy and security threats (Section 2.2), examines context-specific concerns (Section 2.3), and introduces the Contextual Integrity (CI) framework (Section 2.4), which underpins our investigation of privacy perceptions.

2.1 Privacy Concerns of Users in Video Conferencing

Emami-Naeini et al. [17] conducted one of the earliest comprehensive studies examining users' privacy attitudes towards remote communication tools, including video conferencing. The study explored privacy concerns across conferencing tools, communication modes (e.g., camera/microphone use), and home environments in diverse contexts such as business, education, and socialization. The findings revealed that users frequently mention security and privacy as the critical factors in choosing conferencing tools but they often lack autonomy in selecting tools or activating features like cameras and microphones, with such decisions largely dictated by employers or educators. The study also showed that privacy concerns are highly context-dependent and thus vary across social settings, which aligns well with our results; see Section 4. The authors recommended user-centric privacy features and policies to empower privacy-conscious behaviors.

Building on Emami-Naeini et al.'s work, Prange et al. [30] investigated privacy-invasive incidents that occurred during home video conferencing. The study details scenarios where webcams and microphones inadvertently exposed personal information, such as living arrangements, family relationships, and hobbies. Despite employing protective measures like virtual backgrounds, users face persistent privacy risks. The authors proposed proactive strategies to enhance user privacy before, during, and after meetings.

Weinberger et al. [58] expanded on these insights, analyzing privacy, security, and usability perceptions in the use of video conferencing platforms during and after the COVID-19 pandemic. Their findings show that usability is the dominant factor influencing app choice, even over privacy and security. However, users expressed heightened concern about internal threats, such as unauthorized participant recordings, over external threats like hacking.

While these studies provide valuable insights into privacy concerns in video conferencing, they fall short of examining how specific features impact user perceptions or offering actionable guidelines for privacy-enhancing implementations. Understanding these

specific features is essential because users may well have distinct privacy concerns about particular functionalities in video conferencing, as exemplified by several controversial online discussions on the privacy concerns of these specific features; see the Reddit threads on the pinning feature [34–36, 38] (e.g., *"Do people know if you pin their video?"*), attention tracking [37, 39] (e.g., *"If you're using Zoom for work or school, be aware that Zoom has an attention tracking feature"*), spotlighting [40, 43], and meeting recording [41, 42]. Gaining this understanding can also inform the design of safer and more user-centric video conferencing tools. Moreover, although the importance of social context has been noted [17], nuanced privacy concerns tied to interpersonal relationships within each context remain underexplored. To address these gaps, our study investigates user perceptions of specific features — attention tracking, meeting recording, pinning, and spotlighting — to provide a granular understanding of their impact on privacy concerns.

2.2 Privacy and Security Threats in Video Conferencing

Several studies have highlighted privacy and security threats associated with video conferencing tools. For instance, Kagan et al. [21] demonstrated how personal information could be extracted from recorded video streams, and Neustaedter et al. [27] found that blurred backgrounds offered limited privacy protection. Heitmann et al. [19] conducted a systematic security analysis of the two widely used open-source video conferencing systems for research and education, BigBlueButton and eduMEET, uncovering several system vulnerabilities and bugs.

Cryptographic vulnerabilities have also been uncovered. Maleckas et al. [25] exposed flaws in Jitsi's cryptographic implementation, undermining its strong privacy claims. Reisinger et al. [46] conducted a systematic analysis of Unified Communication platforms, identifying risks such as unauthorized access and weak encryption mechanisms.

2.3 Context-Specific Privacy Concerns in Video Conferencing

Privacy concerns vary significantly depending on the context of video conferencing. Studies have shown that users often feel pressured to enable cameras in professional or educational settings [11, 33]. Cohney et al. [14] explored privacy challenges in remote learning, noting tensions between students' privacy preferences and instructors' expectations. Similarly, Balash et al. [4] identified privacy concerns with intrusive online proctoring features, such as webcam monitoring and screen recording. In telemedicine, Bassan [8] highlighted privacy risks associated with relaxed HIPAA regulations during the COVID-19 pandemic, which enabled rapid telehealth adoption but reduced transparency and safeguards. Inspired by these context-aware privacy risk evaluations, we examine privacy perceptions across business, educational, and social settings in our user study.

2.4 Privacy as Contextual Integrity

To understand more nuanced and detailed privacy perceptions for each feature, we adopt the theory of privacy as contextual integrity (CI) [7, 28], which evaluates the appropriateness of information flows based on context-specific norms. CI defines information flows using five parameters: (i) *sender*, (ii) *recipient*, (iii) *information type*, (iv) *subject*, and (v) *transmission principle*. Privacy is maintained when these flows align with contextual norms; violations result in privacy breaches.

CI has been widely applied across various domains such as online proctoring [4], online learning platforms like MOOCs [60], the Internet of Things (IoT) [3, 48], and AI-generated imagery [10] to uncover the contextual privacy norm. Unlike traditional views that consider privacy as a static act of sharing or withholding information, CI views privacy as the appropriate flow of information according to the context [6].

In our study, we apply the CI framework to assess privacy perceptions related to four specific video conferencing features — attention tracking, meeting recording, pinning, and spotlighting — across three social contexts: business meetings, online lectures, and social gatherings.

3 Methodology

We conduct an online survey to examine individuals' privacy perceptions related to specific video conferencing features. To design the survey, we (1) identified the four features of interest (Section 3.1), (2) defined the CI parameters for each feature (Section 3.2.1-Section 3.2.5), (3) generated the descriptions of information flows based on these parameters (Section 3.2.6), and (4) designed the survey (Section 3.3). We then recruited U.S. citizens through Prolific for our online survey (Section 3.4) and analyzed the results (Section 3.5). We also considered potential ethical issues while designing our survey, which we discuss in Section 3.6.

3.1 Four Features of Interest

To investigate feature-specific privacy perceptions, we narrowed down the total of 124 features to a handful that are most likely to raise privacy concerns in most video conferencing platforms based on four criteria[1]. Two researchers deliberated on the feature selection process until reaching a consensus. During this discussion, we excluded other privacy evaluation metrics, such as transparency of data usage, encryption, and data retention, because they do not directly address user privacy concerns.

The four criteria established through this process are as follows:

(1) *Generality.* To select universally adopted features, we focus on those commonly found on the three most popular video conferencing platforms (Zoom, Microsoft Teams, and Google Meet) [9, 29].
(2) *Information flow.* To identify features that potentially share personal information, we focus on those that create outbound flows of personal data (e.g., video/audio feed).
(3) *External control.* To capture risks initiated by others, we focus on features that are initiated or controlled by other participants.
(4) *Increase in information sharing.* Highlighting features that may increase privacy risks, we focus on those that either maintain or increase (but do not decrease) the amount of information shared about a participant.

[1]The full list of features considered for this study, along with the process used to evaluate them, is detailed in Appendix A.

To select the features of interest, we employed a criteria-based filtering process based on the above criteria. Though one method for feature selection could involve asking users about the features they are most concerned about, we decided against conducting a user study, as it could have introduced bias toward more well-known features than lesser-known ones.

The four features that met each of these criteria are as follows:

Attention tracking. This feature allows the meeting host to monitor participants' engagement by detecting when the client application is not the active application on a participant's computer for more than a specified timeout period (e.g., 30 seconds in Zoom). If a participant is detected as inattentive in Zoom, the host may be notified, and the host may receive a report at the end of the meeting summarizing each participant's attentiveness. While this feature was removed from Zoom in April 2020 due to privacy concerns [50], it remains available in certain versions of Webex (such as Webex Training [12] and Webex Events [13]) and may appear in Microsoft Teams in the future [18]. It is also a topic of ongoing research [5, 15, 20, 23] exploring methods to detect participant attentiveness to enhance online learning experiences.

Meeting recording. The meeting recording feature is available in all popular video conferencing platforms such as Zoom, Microsoft Teams, and Google Meet. A host can use this feature to record all audio and visual information visible to the host, including participants' video feeds and voices. While recording, all participants are notified through an on-screen indicator that the session is being recorded. After the meeting, the recorded data is stored either locally on the host's device or in the cloud. In Zoom, the meeting recording feature was updated in May 2021 to provide active voice notifications for all users regardless of their devices and subscription types. Microsoft Teams also requires explicit consent for meeting recording [45], while in Google Meet, recording notifications remain passive without mandatory consent or active audio notification. In our study, we use passive notifications for this feature as a baseline.

Pinning. Pinning is a feature found in all popular video conferencing platforms that allows users to bring a specific participant's video feed to their main screen, making it the primary video feed. Pinning is typically triggered by selecting an option from the drop-down menu or double-clicking on a participant's video feed. Pinning affects only the screen of the user who activates the feature but not the screens of other participants.

Spotlighting. A host can spotlight a specific participant's video feed, making the participant the primary active participant visible to all attendees. Participants are aware that their video feed is spotlighted when it becomes the primary view on their screen, even if they do not activate it themselves. In Zoom and Microsoft Teams, users can remove their spotlighted video after being spotlighted by the host. However, in Google Meet, the spotlighted user cannot intervene on others' screens; they can only remove it from their own view. In our study, we use the form of spotlighting available in Google Meet as a baseline.

3.2 Defining Contextual Integrity (CI) Parameters depending on Social Contexts

The four features described above are utilized across various social contexts, and each context influences the CI parameters (i.e., senders, recipients, subjects, attributes, and transmission principles). To effectively analyze these variations, we define three different social contexts—business meetings, online lectures, and social gatherings. This setup of three social contexts is similar to the one used in Emami-Naeini et al.'s study [17]. Next, we define five CI parameters (Section 3.2.1-Section 3.2.5) and generate descriptions of information flows (Section 3.2.6) by systematically enumerating the social contexts and CI parameters.

To define the five CI parameters for each combination of feature and social context, two researchers first independently identified possible values for each parameter, ensuring that they reflect diverse interactions occurring in various video conferencing environments. Following this, we conducted discussions to refine and finalize these values through consensus. During these discussions, our primary objective was to reduce the overall number of values (to minimize the length of the survey) while maintaining comprehensive coverage of diverse video conferencing scenarios. As a result, some values were removed, while others are consolidated to streamline the analysis.

3.2.1 Sender. We use a single value for the sender parameter across all contexts — the survey participant, referred to as "you" in survey questions. This reflects our research objective: to examine whether participants are willing to share their data under specific conditions.

3.2.2 Recipient. The recipient parameters are defined based on the social roles relevant to each social context, acknowledging the various social relationships without excessive detail in each setting:

Business meeting. Given the hierarchical nature of business meetings, we define the recipient types using three values: *leadership (e.g., a boss)*, a *team member*, and an *external partner*. These categories reflect the varying levels of authority and responsibility within a typical business environment, without delving into too much detail about specific roles (e.g., clients, suppliers, etc.).

Online lecture. In the context of online lectures, where multiple social relationships exist, we define the values of recipient parameter using five categories: an *instructor*, a *teaching assistant (TA)*, a *friend*, an *acquaintance*, and a *stranger*. This range captures the diverse social relationships that can occur in an educational setting.

Social gathering. For social gatherings, we simplify the recipient parameter to a single category: a *friend*. Social gatherings may well involve strangers too; however, we exclude strangers from this social context to clearly differentiate social gatherings from other, more formal contexts (i.e., business meeting and online lecture) and to maintain conceptual clarity.

To define the recipient parameter for the spotlighting feature, we use a single value: *everyone* regardless of social context. This decision is based on the functionality of the feature itself. When a participant's video feed is spotlighted, it becomes the primary view for all participants rather than being directed to specific individuals. Therefore, instead of segmenting recipient types, we use a single value to accurately represent this feature's broad visibility.

3.2.3 Information type. In this study, the information types are specifically defined for each video conferencing feature, with the aim of capturing the primary form of information conveyed through each feature:

Attention tracking. The information type is defined as the *attention status* of the participant, indicating whether the participant is actively focusing on the Zoom screen during the video conferencing.
Meeting recording. This feature enables the host to record their screen and it involves participants' *audio-visual data*.
Pinning. The information type for pinning is defined as an *enlarged video feed* (referred to as the pinned video feed), which highlights a particular participant's video, making it more prominent on the screen.
Spotlighting. Similar to pinning, the spotlighting feature focuses on an *enlarged video feed* (referred to as spotlighted video feed), which is used to emphasize one participant's video feed for all attendees.

3.2.4 Subject. As with the *sender*, the subject is defined as the participant referred to as "you" in the survey. While it is possible for other individuals to be inadvertently included in the video or audio during conferencing (e.g., those in the same room or within the range of the camera and microphone), our study focuses exclusively on the participant who is intentionally visible/audible. Therefore, only this single subject is considered within the scope of this study.

3.2.5 Transmission principles. To define the transmission principles applicable to our study in a systematic and comprehensive manner, we begin by examining the General Data Protection Regulation (GDPR) [55], now serving as a global data protection regulation [47]. Specifically, we focus on 'Chapter 2 Principles' and 'Chapter 3 Rights of the Data Subject' as these sections outline the principles of personal data processing and the rights for the data owner.

From GDPR, we identify and adapt relevant content for the video conferencing context, organizing them into seven distinct categories: *consent, storing period, management of personal information, notification of data usage, data sharing, purpose of data usage* and *data anonymization*. For instance, the GDPR's lawfulness principle states that consent is required to process data lawfully, which we adapt to the *consent* principle in our transmission principles. Similarly, we draw our *storing period* principle from the principle of storage limitation in Chapter 2 in [55], which mandates that personal data should only be stored for as long as necessary. Chapter 3 [55] emphasizes that information should be provided when personal data is collected from the data subject, which informs our *notification of data usage* and *purpose of data usage* principles.

In addition to these seven categories, we introduce an extra contextual factor termed *situational context*, which takes into account the composition of meeting participants and specific relevant condition. This allows us to formulate diverse transmission principles that reflect real-world user perceptions, which are not directly addressed in GDPR.

Based on these eight categories, we systematically formulate transmission principles relevant to each feature, social context, and recipient. Two researchers collaboratively worked on constructing generalizable scenarios, ensuring that the principles capture a diverse range of realistic situations while they are not overly detailed. When disagreements arose, we prioritized reducing the overall number of parameters.

Table 1 shows the transmission principles we use for the *attention tracking* feature as an example. The *storing period* category is formulated to include statements like "*If the data is not stored and only used during the meeting*," " *If the data is destroyed after a week*" and " *If it's unknown for how long the data is stored.*" We have excluded some combinations that are nonsensical or irrelevant. For instance, we exclude the social gathering context (hence presenting only two columns of social contexts) as it would be unusual for a host to monitor their friends' attention during a gathering intended for socializing and entertainment. We also exclude "*used for meeting review*" and "*used for AI training*" because these are irrelevant to the use of the attention tracking feature.

We apply this transmission principle definition process across three additional features (i.e., meeting recording, pinning, and spotlighting), with full details provided in Appendix C.

3.2.6 Generating Descriptions of Information Flows. Based on these CI parameters, we generated 219 distinct descriptions of information flows that are tailored for each social context and feature. To explore the impact of social contexts and varying CI parameters on each video conferencing feature, we then asked participants to rate how acceptable they find the information flows.

The first question each participant answered was the baseline question. *Baseline questions* ask about the acceptability of each feature when triggered by a specific *recipient* within a particular *social context*, *without* considering any transmission principles. The template for the baseline question is:

> *"You are participating in a [social context] through a video conferencing platform. How acceptable is it for you when [recipient] [triggers a feature] and [information type] is shared with [recipient]?"*

Note that we modified each statement slightly to prevent any misunderstanding; e.g., *"You are participating in an online lecture through a video conferencing platform. How acceptable is it for you when the instructor tracks your attention during the online lecture?"* (see Appendix D.3.1 for the full set of baseline questions.)

After the baseline questions, participants were then asked to rate the acceptability of full descriptions of the information flows including transmission principles; see Appendix D.3.2 for the full set of questions). For example, participants were asked:

> *"You are participating in a [social context] through a video conferencing platform. How acceptable is it for you when [recipient] [triggers a feature] and [information type] is shared with [recipient] under the [transmission principle]?"*

To fill out the template, we systematically applied the structure outlined in Table 1 and Table 4–6 in Appendix C. By enumerating all defined information flows, we constructed descriptions that serve as the basis for the survey questions.

3.3 Survey Design

Survey participants were asked to rate how acceptable they find the information flows generated in Section 3.2. Since asking participants to evaluate all 219 information flows likely results in mental fatigue, reducing the reliability of their responses, we divided the entire information flow set into seven smaller subsets, each designed

			Social Contexts and Recipients				
			Business meeting			Online lecture	
			Leadership (e.g., boss)	Team member	External partner	Instructor	Teaching assistant
Categories from GDPR and Transmission Principles	Consent	Explicit consent required	If you have given explicit consent for tracking your attention and approve it				
	Storing period	Data not stored	If the data is not stored and only used during the meeting				
		Data stored short period	If the data is destroyed after a week			If the data is destroyed after the semester	
		Storage duration unknown	If it's unknown for how long the data is stored				
	Notification of data usage	Notification on tracking	If there is a notification when your attention is tracked				
	Data sharing	Shared privately	If the attention data of you is shared within your team			If the attention data of you is shared within the class	
	Purpose of data usage	Real-time tracking	If the attention data is used to monitor your real-time attentiveness during the meeting				
		Used for evaluation	If the attention data is Used to grade your performance based on attentiveness	n/a	n/a	If the attention data is used to grade your attentiveness	
		Used for feedback	If the attention data is used to provide feedback to the leadership (e.g., your boss) and enhance future business meetings	n/a	n/a	If the attention data is used to provide feedback to the lecturers and improve future lectures	
	Anonymization	Anonymized data to host	If the attention data of all participants is aggregated and presented to the *[recipient]* as a single percentage				

Table 1: Table of transmission principles for *attention tracking*. We draw transmission principles from an understanding of social contexts, recipients, and also from relevant GDPR principles.

to take approximately 5 minutes to complete. To ensure consistency in participants' experiences of video conferencing within a specific social context, we avoided random assignment and instead grouped participants systematically. Each participant was assigned to one subset, with groups evaluating from 26 to 35 information flows with an average of 31 flows per subset. Details for the information flow distribution across survey groups can be found in Table 3.

3.3.1 Introduction, Screening, and Feature Overview. At the beginning of the survey, participants were provided with an overview of the survey's purpose, the expected time commitment (i.e., 5 minutes on average), and assurances that their data would be anonymized and then destroyed after the research was complete.

Then, participants were required to verify their video conferencing experience in the specified social context through a screening question, with those lacking relevant experience being excluded from the survey; see Appendix D.1. For participants who passed the screening, we provided information about each video conferencing feature to ensure consistent understanding, withheld specific details to avoid bias, and asked about their prior experience with the features; see Appendix D.2.

3.3.2 Contextual Integrity Statements. We then asked participants to answer how acceptable they find the subset of information flows generated in Section 3.2.6. The acceptability score was rated on a 5-point Likert scale: (1) Completely unacceptable; (2) Unacceptable; (3) Neutral; (4) Acceptable; and (5) Completely acceptable. Participants were required to answer all questions before proceeding to the next step. We implemented this approach to ensure complete responses, allowing for direct comparisons across participants with an identical number of data points.

First, the participants were asked baseline questions to determine their privacy perceptions regarding each social context and recipient; see Appendix D.3.1. The responses also provide a reference point for comparison within information flows with specific transmission principles.

After completing the baseline questions, participants were asked to answer the acceptability for the complete CI statements, including the transmission principles; see Appendix D.3.2. The order of the statements was randomly shuffled to avoid habituation bias.

3.3.3 Demographics. At the end of the survey, we collected information about demographic characteristics including gender and age, to better understand the diversity of our participant sample; see Appendix D.4.

3.4 Recruiting Participants

The survey was developed and administered through Qualtrics [32], with participant recruitment facilitated by Prolific [31], an online platform that enables researchers to efficiently distribute surveys to a large and diverse population. We required participants to be U.S. citizens to minimize the influence of factors such as cultural differences on the survey results. Our recruitment goal was to recruit at least 100 participants for each group, ensuring a fair and inclusive gender distribution across all groups. We also prevented participants from completing the survey more than once by using Prolific's prescreening option, ensuring no overlap between groups. The survey took approximately 5 minutes to complete, and 769

participants were compensated £0.75, which was the recommended compensation rate on Prolific.

3.5 Data Analysis

For the analysis, we focused on the influence of social context and CI parameters (recipients and transmission principles) on the perception of each video conferencing feature. To observe general trends, we first calculated the average acceptability score for each baseline statement. We then compared the impact of social contexts and recipients on each feature, as well as the overall trends in acceptability across different recipients and features.

We also examined how the application of transmission principles affects the acceptability for each feature under each recipient type. With all the other factors except for the transmission principles (i.e., feature, social context, and recipient) being fixed, we compared the effect of transmission principles against the baseline by verifying the statistical significance between the two datasets. Since the transmission principle questions were asked to the same participants who answered the baseline questions, we treat the responses as paired data. We used the non-parametric Wilcoxon signed-rank test [59] to assess the differences.

Since we conducted multiple tests, we accounted for the Family-Wise Error Rate (FWER). We apply the Holm-Bonferroni method [1], which adjusts the significance threshold for each hypothesis test in a stepwise manner, controlling for multiple comparisons.

In addition to the contextual integrity factors, we also searched for any other factors that affect the privacy perception of video conferencing features. To determine whether this factor contributes to a significant difference in acceptability scores between two independent groups, we conducted a Mann-Whitney U test [26] to verify if the factor contributes to any significant difference in the acceptability scores between two independent groups.

3.6 Ethical Considerations

This study, including its consent, recruitment procedures and survey, was reviewed and approved by our institutional review board (IRB). Participants were informed of the study's purpose and topic at the beginning of the survey and were free to withdraw at any time. Additionally, they were notified that they could be screened out if they did not meet the eligibility criteria. All data was anonymized and identified using random identifiers to ensure participant privacy.

4 Findings

In this section, we present the results of our user study. After summarizing the participants' demographics (Section 4.1), we present the general trends of the results of the baseline questions (Section 4.2). We then show the impact of transmission principles on the acceptability of the four features of interest (Section 4.3). Finally, we describe how several other notable factors affect the acceptability of information flows, such as gender and prior experience (Section 4.4).

4.1 Demographics

As shown in Table 3 in Appendix B, participants were divided into seven separate groups based on the criteria described in Section 3.3. Each group had 100 or more participants, with 769 participants in total. Among them, 385 were male, 364 were female, and 20 preferred to self-describe. The age of the participants ranged from 18 to 79 years (mean = 35.25, median = 33.0, std. deviation = 11.83). Those who were asked about the online lecture context (Groups 4, 5, and 6) tended to be younger (average = 32.36) than the groups answered the social gathering context questions (Group 7, average = 36.10) and the business meeting context questions (Groups 1, 2 and 3, average = 37.73).

4.2 General Trends: Analysis of Baselines

To understand the general trends in participants' responses, we compare the average acceptability scores of the baseline questions in Figure 1. First, we examine the acceptability scores of baseline questions to compare different features, social contexts, and recipients. Next, we analyze how transmission principles influence these baseline scores.

Comparison among features Among the four different features, meeting recording consistently shows the highest acceptability scores across all recipient types, whereas attention tracking consistently shows the lowest. A notable observation is that two of the lowest values are found for the *team member* recipient category for attention tracking and the *stranger* category for pinning, both scoring slightly above 2 (unacceptable). This indicates that when the pinning feature is used by strangers, users' discomfort can be as significant as with attention tracking, which had been removed from Zoom due to privacy concerns.

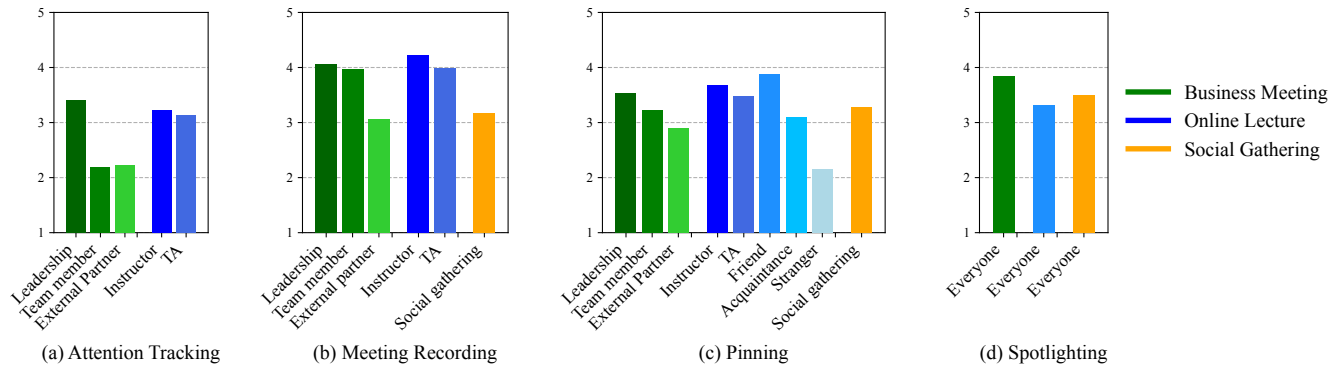
Comparison among social contexts The social context itself has a relatively smaller impact on privacy perceptions, while acceptability scores vary significantly based on relationship dynamics within each social context.

Comparison among recipients Comparing acceptability among recipients, participants generally found the features more acceptable when used by authorized or familiar individuals. For instance, the acceptability of the removed attention tracking feature is close to neutral (3) when utilized by an instructor or teaching assistant (TA) in an online lecture context, or by leadership in a business meeting context. In contrast, acceptability declines significantly when the feature is used by a team member or an external partner in a business meeting context. This trend is consistent across all features and social contexts.

Application of transmission principles We evaluated the responses of the participants when privacy-preserving transmission principles were applied; see Figures 2– 7. Overall, implementing privacy measures significantly reduced the gap in privacy concerns between different recipient types within the same social context. Notably, obtaining user consent before enabling a feature emerged as the most effective strategy to increase acceptability. Participants also felt more comfortable when they had greater transparency about when and how their information would be used, as well as greater control over its usage.

4.3 Comparison among *Transmission Principles*

This section details the results from the transmission principle questions, asking about the acceptability of a specific information flow given the transmission principles. We examine the relative



(a) Attention Tracking (b) Meeting Recording (c) Pinning (d) Spotlighting

Figure 1: Average acceptability scores of baseline questions across different social contexts and recipients for (a) attention tracking, (b) meeting recording, (c) pinning, and (d) spotlighting. The acceptability scores range from 1 ("completely unacceptable") to 5 ("completely acceptable").

effect of transmission principles by comparing the acceptability scores with those of the baseline questions. That is, a transmission principle (e.g., *explicit consent required, data not stored,* and *shared privately*) can be interpreted to have a positive effect when the acceptability score is higher compared to the baseline.

4.3.1 Attention Tracking. Figure 2 shows the acceptability scores of the attention tracking feature, across different transmission principles.

The transmission principle of *explicit consent required* substantially increases the acceptability of the attention tracking feature. Additionally, we observe that acceptability tends to increase under the principles of *data not stored*, *data stored short period*, *notification on tracking*, and *anonymized data to host*, which enhance privacy. The acceptability is also influenced by the purpose of attention tracking; acceptability increases under transmission principles of *real-time tracking*. In contrast, the principles of *storage duration unknown*, *shared privately*, and *used for evaluation* tend to reduce the acceptability scores.

While the transmission principles of *data not stored*, *data stored short period*, and *real-time tracking* generally increase acceptability, they show a decline when the recipient is leadership within a business meeting context. One possible explanation is a limitation of the survey design, which made it difficult to compare the acceptability of transmission principles with the baseline question. This challenge arises because the two types of questions were structured differently. In the baseline questions, participants compared the relative acceptability of different recipients. In contrast, the transmission principle questions required participants to evaluate the acceptability of each principle relative to one another, but only for a specific recipient type.

Takeaways: attention tracking. While users tend to agree that the attention tracking feature could be unacceptable in many contexts, hence justifying its removal, the study also found that the feature can be much more acceptable when used with care. Users express neutral feelings when the feature is activated by the instructor or TA in an online lecture context or by leadership in a business meeting context. However, privacy concerns do exist, particularly when it is used by less directly authoritative persons (e.g., team members and external partners in business meeting contexts). The discomfort becomes severe when the users are unaware of how long the data is stored and shared with others.

4.3.2 Meeting Recording. As shown in Figure 5 in Appendix E.1, applying transmission principles generally had negative effects on acceptability of the meeting recording feature. Notably, the principle of *explicit consent required* emerges as the most effective in enhancing the acceptability of the meeting recording feature across diverse recipient types. Participants tended to demonstrate decreased acceptability for transmission principles including *storage duration unknown*, *shared publicly*, *data anonymized*, or data modification such as *audio not recorded*, *video not recorded*, *video blurred*, or *voice modulated*. The principle of *no notification given* significantly lowers the acceptability.

Transmission principles involving specific purposes, such as *used for profiling*, *used for AI training*, *used for fun*, *used for evaluation* also lead to decreases in acceptability. While the transmission principle of *shared privately* decreases acceptability when used by leadership in a business meeting, instructor in an online lecture, or a friend in a social gathering, it increases when used by an external partner in a business meeting. This result could also have been influenced by the limitation of our survey design, as discussed earlier in 4.3.1.

Takeaways: meeting recording. The update of the meeting recording feature by Zoom, requiring recording consent and active notifications, seems to be an effective way to improve privacy. Yet, there are still concerns about how long the data will be stored and the scope of data sharing. In particular, publicly sharing recorded data may cause

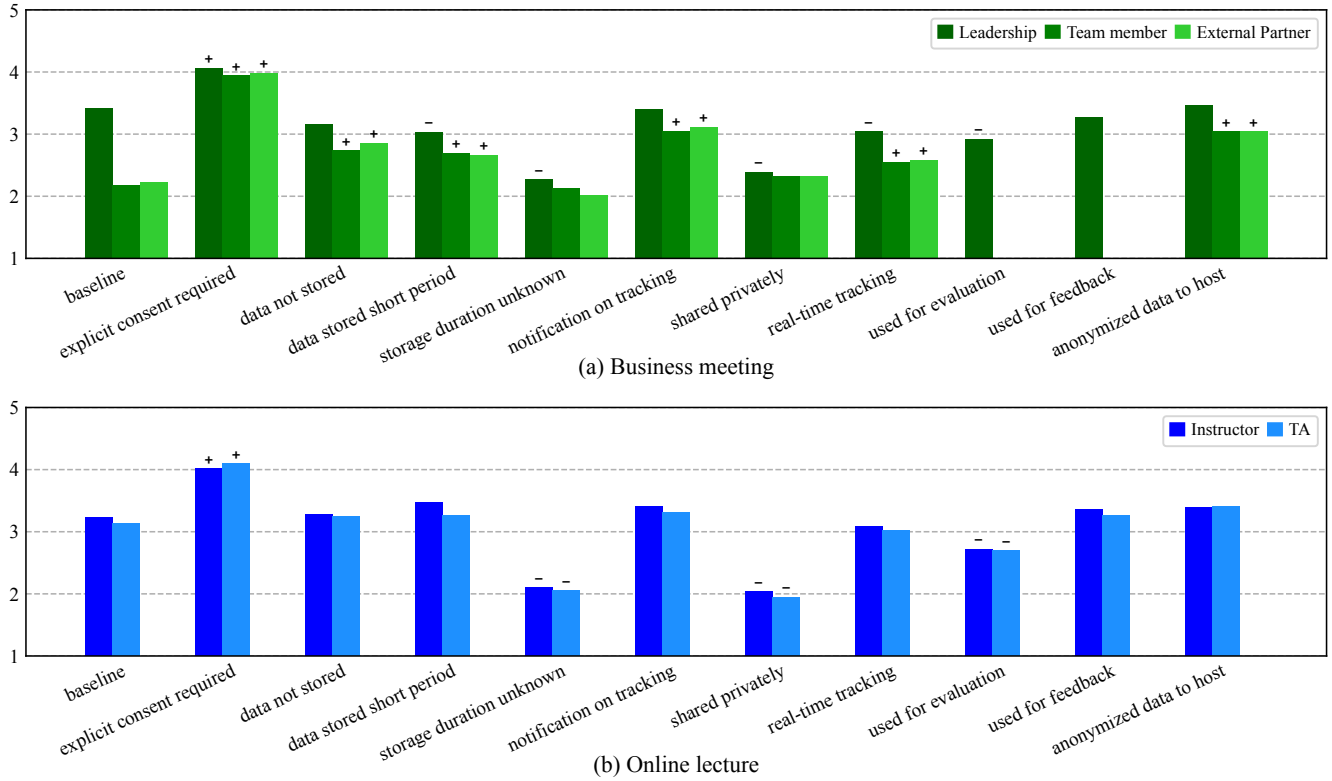


Figure 2: Average acceptability scores for the attention tracking feature on baseline and transmission principle conditions, across different recipients in social contexts of (a) business meeting and (b) online lecture. The '+' and '–' marks indicate the statistical significance of $p < 0.05$, where '+' and '–' indicate the acceptability score being higher and lower than the baseline, respectively.

significant discomfort. This shows that the recording feature still poses a potential privacy problem. Our findings suggest that data modifications such as blurring video, modulating audio, or including only video or only audio to enhance privacy fail to effectively address privacy concerns. Likewise, anonymizing data appears insufficient in alleviating participants' apprehension about their privacy.

4.3.3 Pinning. As shown in Figure 6 in Appendix E.1, the effect of transmission principles on the acceptability of pinning is consistent across different social contexts. *Explicit consent required* and *receive notification when pinned* substantially increase the acceptability of pinning. In addition, the transmission principles *option to control feed size* and *option to control pinning time limit* tend to have a positive effect on acceptability, though they have a negative effect when pinning is used by a friend in an online lecture context.

The principle of *pinned while speaking* significantly increases the acceptability of pinning, whereas the acceptability diminishes with the principle of *pinned while muted*. The use of *forced to turn on camera* also negatively impacts acceptability. Prior work [17] highlights that participants often experience a lack of autonomy when using webcams in video conferencing. This lack of autonomy, as demonstrated in this work, can further exacerbate discomfort associated with pinning.

Takeaways: pinning. The privacy acceptability of the pinning feature varies significantly depending on the recipient type within each social context. Users generally feel more comfortable when pinned by individuals who are familiar or who have authority. Conversely, discomfort intensifies when users are pinned by strangers, particularly in an online lecture setting, where these individuals are both unfamiliar and lack authority. The acceptability scores in these cases are the lowest across all the questions we test in this study.
Participants also express a strong preference for autonomy and control over their visibility during online interactions, emphasizing the importance of not being forced to activate their cameras.

4.3.4 Spotlighting. As we show in Figure 7 (in Appendix E.1), the acceptability of being spotlighted tends to increase as a result of transmission principles such as *explicit consent required*, *spotlighted while speaking*, and the ability, *can remove spotlight*. In contrast,

acceptability diminishes under the *spotlighted while muted* transmission principle and in specific situations such as *majority are supervisors* or *majority are external partners* in business meetings. Acceptability of transmission principles like *option to control feed size* and *option to control spotlight time limit* decrease in business meeting, while that of *option to control spotlight time limit* increases in a online lecture context. Additionally, the acceptability of *data anonymized* decreases in a business meeting.

Takeaways: spotlighting. Spotlighting is generally perceived as more acceptable to participants than pinning. Yet, privacy concerns arise when participants are spotlighted while muted. In addition, the composition of the participant group in the meeting affect the acceptability; e.g., if the majority of participants are unfamiliar or less authoritative, such as supervisors, external partners in business meetings, the opposite sex in online lectures, or acquaintances in social gatherings, the discomfort increases.

4.4 Two Other Factors: *Gender* and *Prior Experiences*

In this section, we investigate how gender and prior experience further affect the acceptability of information flows. In our work, unfortunately, we are not able to not analyze the impact of age because of a significant imbalance across age groups, as we lacked older participants with certain video conferencing experiences, such as online lectures.

4.4.1 Gender. Gender shows a significant difference in privacy perception between different groups. Participants identified their gender as male, female, or other. Due to the small number of participants who chose to self-describe as others (see Table 3 in Appendix B), we only focus on the male and female groups.

Among the four features we examined (attention tracking, meeting recording, pinning, and spotlighting), the information flows of the meeting recording and pinning feature show significant differences between the two gender groups. The other two features show little or no difference in acceptability between the two groups.

Figure 3 shows the average acceptability scores for the given information flows by gender regarding the meeting recording feature. Overall, female participants show lower acceptability scores compared to the male participants. The gap becomes more significant with certain transmission principles, including *data stored short period*, *storage duration unknown*, *audio not recorded*, *voice modulated*, *no notification given*, *shared publicly*, *data anonymized* and *three secondary usage conditions*. The same trend is observed with the pinning feature, where female participants find it less acceptable than male participants. Further details are provided in Figure 9 in Appendix. The other two features, attention tracking and spotlighting, show relatively little difference across gender groups; see Appendix E.2.

4.4.2 Prior Experience. Participants were grouped based on their prior experience with each feature: (1) those who had not previously been aware of the feature, (2) those who had heard of it but never used it, and (3) those who had used it; see Appendix D.2. In the case of attention tracking, participants were categorized as either having heard of the feature or not, as the feature has been removed from Zoom.

For the pinning and spotlighting feature, participants were relatively evenly distributed over the different groups. However, for the other two features, the number of participants was very unevenly distributed, making it inappropriate for comparison; hence, we omitted the results. This disparity may be due to the unfamiliarity of the attention tracking feature, as it is currently unavailable on most platforms, and the widespread usage of the meeting recording feature, which is not only commonly used but also prominently notifies users of its presence, reminding them of its functionality.

Figure 4 shows acceptability scores of participants based on their level of prior experience with the pinning feature. Overall, participants with prior experience generally exhibited *higher* acceptability scores for transmission principles compared to those with no experience or knowledge of the feature. This trend is evident across various contexts, particularly in business meetings involving *leadership*, *team members*, and *external partners*, as well as in social gatherings involving *friends*. Transmission principles where significant differences are found include *control over feed size*, *control over pinning duration*, *notification upon being pinned*, *pinned while speaking*, and *pinned while muted*.

The spotlighting feature exhibits a similar trend, with participants who have prior experience with it showing higher acceptability compared to the other two groups in most cases; see Figure 13 in Appendix E.

5 Discussion

5.1 Rethinking Privacy in Video Conferencing

Building on prior work that broadly examined privacy concerns in video conferencing, this study contributes to the literature by shifting the focus toward specific features and their associated privacy implications. We uncover nuanced privacy concerns by analyzing how different relationships influence privacy perceptions and identifying the conditions under which these concerns are either heightened or mitigated.

Our study shows that the traditional understanding of privacy [11, 33] falls short in reflecting how users perceive privacy issues in real-world video conferencing. Previous research revealed that users are often hesitant to turn on their cameras during online meetings or classes, with privacy concerns predominantly framed around the binary question of whether the camera is on or off. Yet, such a coarse-grained view fails to capture the nuanced privacy concerns surrounding specific features like pinning or spotlighting.

Many participants in our study indeed felt that actions like pinning or spotlighting are privacy-invasive, even when their cameras were turned on; see Section 4.3.3 and Section 4.3.4. This suggests that visibility is not merely about *being seen* — it also involves being constantly and prominently visible through an enlarged video feed, which effectively singles out individuals from the group of participants. Moreover, their privacy perceptions are shaped by factors such as social relationships, degrees of closeness, and hierarchical dynamics among participants.

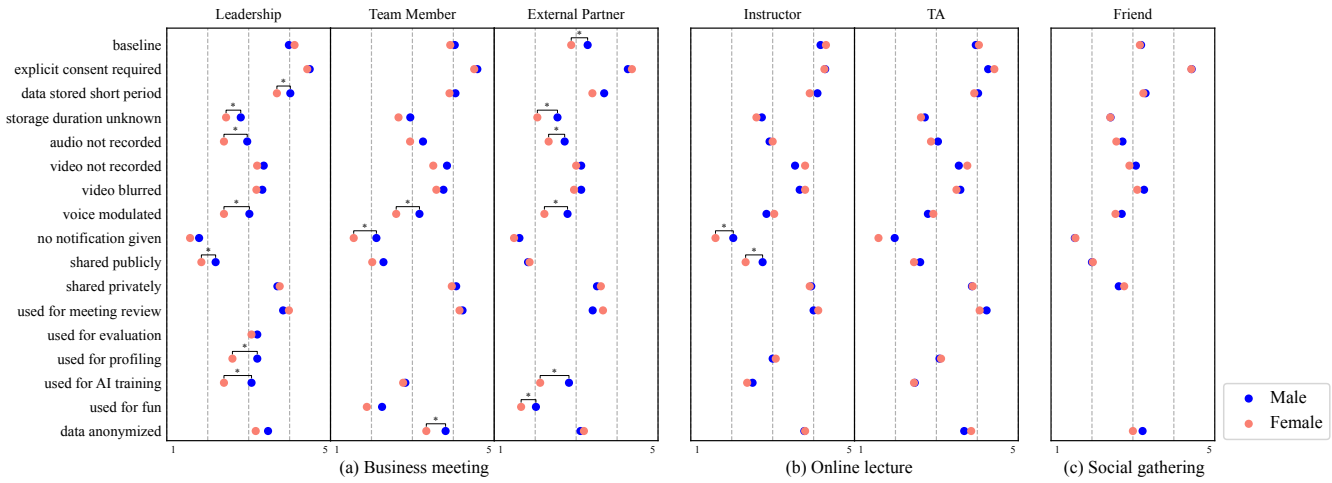


Figure 3: Average acceptability scores for the meeting recording feature by gender groups, for the given transmission principle (left) and recipient type (top), in the social context of (a) online lecture, (b) business meeting, and (c) social gathering. (*) indicates statistical significance, with $p < 0.05$.

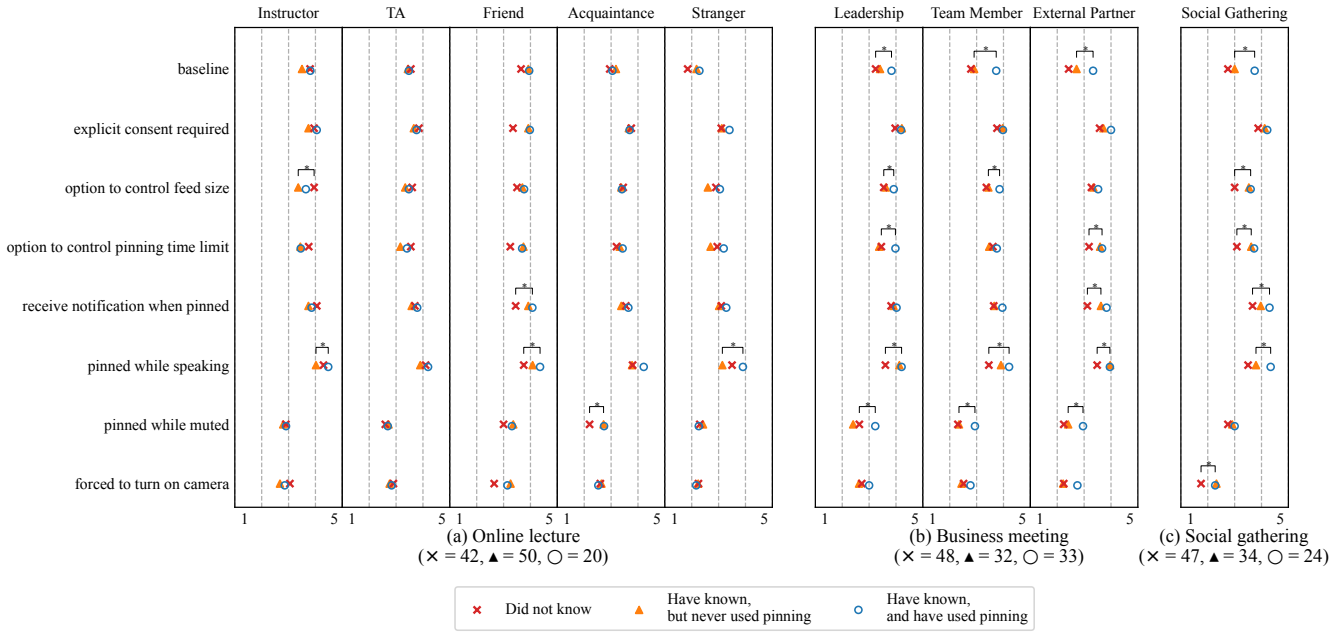


Figure 4: Average acceptability scores for the pinning feature by participants with different prior experiences, for the given transmission principle (left) and recipient type (top), in the social context of (a) online lecture, (b) business meeting, and (c) social gathering. Parentheses indicate the number of participants in each group. (*) indicates statistical significance, with $p < 0.05$.

This discrepancy highlights the need to rethink privacy in video conferencing. What might have seemed non-invasive under traditional views can still feel invasive to users, especially when social contexts and power dynamics are taken into account. For this investigation, the privacy framework of contextual integrity (CI) [28] allowed us to effectively capture users' privacy concerns in different features and social contexts. Overall, our findings emphasize the need for a more nuanced, context-sensitive approach to understanding the diverse privacy concerns users encounter in video conferencing settings.

5.2 Design Recommendations

While our study highlights the current state of privacy perceptions in video conferencing, it also provides valuable insights about which transmission principles can enhance the acceptability of the features we studied. Based on our findings, we propose several possible design recommendations.

Attention tracking. We confirmed that the previous design of the attention tracking feature can raise privacy concerns, particularly when used by unauthorized individuals (e.g., team members or external partners in business meetings). Additionally, privacy concerns may arise if the host does not clearly explain how long attention data will be stored, whether it will be shared, or if it will be used for evaluations.

Based on our observations on several transmission principles that help to increase the acceptability of the attention tracking feature, we propose several design recommendations. First of all, transparency is key to addressing privacy concerns. Users want to know how their data is being stored and used. This could be achieved by providing real-time notifications when attention tracking is active and by obtaining explicit consent for both tracking attentiveness and data storage duration.

Second, we also recommend anonymizing attention data, possibly by presenting it as aggregated statistics rather than individual status. While our survey suggests that this approach could mitigate privacy concerns, it also reduces data granularity, which may limit its usefulness for meeting hosts. Further studies are needed to explore this trade-off in order to identify the balance between usability and privacy.

Additionally, restricting the use of the attention tracking feature to authorized groups, such as those with instructor or business accounts, could help alleviate privacy concerns. Our findings indicate that participants feel relatively more comfortable when the feature is used by authorized individuals. Authorized accounts could serve as proxies for authorized persons, helping to reduce the risk of misuse or abuse of the feature.

Meeting recording Popular video conferencing platforms such as Zoom, Microsoft Teams, and Google Meet notify users when a meeting is being recorded. While these notifications help to increase the acceptability, concerns remain regarding how long recordings are stored, how they are shared, and how they are used. Similar to attention tracking, people are particularly worried when there is uncertainty about how long their recorded data will be stored and whether it could be shared publicly.

To address these concerns, we suggest a few solutions. First, for platforms that already require consent for recording, such as Zoom and Microsoft Teams, the consent prompt might include clear information about storage duration and data sharing practices. One possible implementation is to allow the host to specify, at the time of initiating a recording, the duration for which the data will be stored and who will have access to it. This information would then be displayed to all participants, enabling them to provide informed consent.

Second, platforms could implement cloud storage solutions with clear restrictions on data sharing and pre-determined timeframes for how long the data will be kept. This approach must be designed with caution though, as involving third-party platforms in the storage and sharing of data could introduce additional privacy concerns. Transparent policies and robust safeguards would be critical to ensure users' trust and data security.

Pinning. Our baseline survey shows that privacy concerns arise when users are pinned by unfamiliar individuals, such as strangers in an online lecture or external partners in a business meeting. These concerns are heightened when participants are pinned while muted, making it difficult for them to understand the reasons behind the pinning. Additionally, being forced to turn on their camera increases privacy worries.

To mitigate these concerns, several measures can be considered. First, pinned users are often unaware of how their enlarged video feed is being used. Providing notifications when their feed is pinned might help. These notifications yet should be carefully designed to avoid disrupting the virtual meeting experience. For instance, excessively frequent notifications could harm usability. A balanced approach could involve subtle visual indicators, such as small emojis or icons on the video feeds of users who pin, to inform participants without overwhelming them.

Second, pinned users lack control over their video. Offering options to limit the size of the pinned feed or how long it can be pinned would give users more control. For example, participants could configure maximum allowable sizes and time limits for their pinned feed through a settings page. The system should enforce minimum values for both size and duration to ensure that the pinning functionality—designed to provide a larger view of specific participants—is not rendered ineffective. Additionally, clear communication about these new features should be provided to all users, especially those who can pin, to prevent confusion when using this functionality.

Finally, obtaining consent before someone can pin a participant's video feed might further enhance privacy. Requiring explicit consent for every instance of pinning may be burdensome and could negatively affect usability. Thus, a more practical approach would be to gather consent regarding pinning permissions when participants first join the meeting. This approach could balance privacy with usability while reducing the need for repetitive consent requests.

Spotlighting. Overall, the current design of spotlighting is generally acceptable to most users. However, privacy concerns tend to increase depending on who is present in the meeting. For example, concerns are higher when the majority of participants are supervisors or external partners in a business meeting, members of the opposite sex in an online class, or acquaintances in a social gathering.

Video conferencing platforms like Zoom and Microsoft Teams currently offer an option to remove the spotlight immediately after a user's video is spotlighted for everyone, which can be a helpful privacy-enhancing feature for others. Additionally, we suggest that obtaining explicit consent before spotlighting someone's video could further improve user comfort with this feature.

5.3 Broader Implications

5.3.1 Gender Differences for Privacy Research in Video Conferencing. Gender differences play a significant role in shaping privacy

perceptions in video conferencing; see Section 4.4.1. Overall, female participants rated a variety of scenarios as less acceptable from a privacy perspective, particularly for the meeting recording and pinning features. This finding aligns with prior research [54], which demonstrated that female participants exhibit higher privacy concerns and display more cautious privacy behaviors compared to male participants. Future research could further explore gender differences in privacy studies within video conferencing contexts in order to identify more inclusive privacy solutions.

5.3.2 Proactive Approach for Feature Development. In the past, features such as the attention tracking feature have been removed or modified reactively in response to user privacy concerns. To address privacy concerns more proactively, it is crucial to collect early feedback from users before fully deploying a feature. This can be achieved by recruiting participants from regular platform users, providing them access to beta versions of features, and incorporating their feedback into the development process.

5.4 Limitations

In our exploration of user privacy concerns with video conferencing features, we identified a significant gap between the design of current features and user privacy expectations. However, due to the scope of our research and the constraints of the survey methodology, our focus was limited to the specific research questions we selected. In the following, we discuss the limitations of this study and outline several directions for future research.

- While our criteria for feature selection (see Section 3.1) were chosen to highlight features likely to raise privacy concerns, they do not encompass all features users might find worrisome. Applying alternative criteria could help identify additional features not addressed in this study.
- When defining CI parameters, we were unable to enumerate all possible variations due to the diverse and complex nature of real-world scenarios. Social relationships often have ambiguous boundaries, making it difficult to establish universally applicable categories. As a result, some aspects may have been oversimplified. However, we prioritized reducing the total number of CI parameters, as this directly impacts the total number of survey questions and helps mitigate participant burden.
- While surveys provide valuable insights, they have a few methodological limitations. Since we solely rely on participants' self-reported responses, there may be discrepancies between their reported attitudes and actual behaviors. Incorporating observational or experimental methods, such as analyzing real-world interactions on video conferencing platforms, could have provided more comprehensive data to validate and enrich the survey findings.
- The use of 5-point scales for acceptability assessment in our CI framework may not fully capture the underlying privacy concerns. Including open-ended questions to collect text-based responses could be a promising direction for future research. Furthermore, we prioritized reducing survey fatigue by minimizing the number of questions. However, this may limit the depth of responses.
- Crowdsourcing platforms provide access to large and diverse populations and are commonly used to gather security and privacy attitudes [16, 44, 56]. We chose Prolific for its higher data quality compared to other platforms [53]. However, our participant pool primarily comprised individuals from the United States, which constrains the generalizability of our findings.

6 Conclusion

This work seeks to highlight the disconnect between users' privacy expectations and concerns regarding various features in video conferencing platforms and how these platforms' existing features fail to reflect the complexity of users' privacy perceptions. Given the evidence of this gap, we advocate for more extensive research built on context-specific notions of privacy, and we encourage platform operators to take a more proactive approach in understanding user privacy perceptions.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable comments and suggestions. The authors used ChatGPT4o to revise the text, correct any typos, grammatical errors, and awkward phrasing. This work is supported by the National Research Foundation of Korea (NRF) and the Ministry of Science and ICT (MSIT) under grant RS-2024-00464269.

References

[1] Hervé Abdi. 2010. Holm's sequential Bonferroni procedure. *Encyclopedia of research design* 1, 8 (2010), 1–8.
[2] CGTN America. 2022. 2020's Most embarrassing Zoom moments. https://www.youtube.com/watch?v=yZpEpNPaxsw.
[3] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents'{IoT} Toy Privacy Norms Versus {COPPA}. In *28th USENIX security symposium (USENIX security 19)*. 123–140.
[4] David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv. 2021. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Seventeenth symposium on usable privacy and security (SOUPS 2021)*. 633–652.
[5] Luis Barba-Guaman and Priscila Valdiviezo-Diaz. 2022. The attention of students in online education: Using head pose techniques to detect attention in videoconferencing platforms: A case study. *International Journal of Emerging Technologies in Learning (Online)* 17, 22 (2022), 144.
[6] Louise Barkhuus. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 367–376.
[7] Adam Barth, Anupam Datta, John C Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. In *2006 IEEE symposium on security and privacy (S&P'06)*. IEEE, 15–pp.
[8] Sharon Bassan. 2020. Data privacy considerations for telehealth consumers amid COVID-19. *Journal of Law and the Biosciences* 7, 1 (2020), lsaa075.
[9] Sunny Betz. 2023. 16 video conferencing platforms keeping us connected while apart. https://builtin.com/articles/video-conferencing.
[10] Natalie Grace Brigham, Miranda Wei, Tadayoshi Kohno, and Elissa M Redmiles. 2024. "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery. *arXiv preprint arXiv:2406.05520* (2024).
[11] Frank R Castelli and Mark A Sarvary. 2021. Why students do not turn on their video cameras during online classes and an equitable and inclusive plan to encourage them to do so. *Ecology and Evolution* 11, 8 (2021), 3565–3576.
[12] Webex Help Center. 2018. Track participant attention in Cisco Webex training. https://help.webex.com/en-us/article/st7tr1/Track-Participant-Attention-in-Cisco-Webex-Training.
[13] Webex Help Center. 2021. Track participant attention in Webex events. https://help.webex.com/en-us/article/yj9y4z/Track-Participant-Attention-in-Webex-Events-(Classic).
[14] Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider, and Madelyn Sanfilippo. 2021. Virtual classrooms and real harms: Remote learning at {US}. universities. In *Seventeenth*

Symposium on Usable Privacy and Security (SOUPS 2021). 653–674.
[15] Mohamed Elbawab and Roberto Henriques. 2023. Machine Learning applied to student attentiveness detection: Using emotional and non-emotional measures. *Education and Information Technologies* 28, 12 (2023), 15717–15737.
[16] Pardis Emami-Naeini, Joseph Breda, Wei Dai, Tadayoshi Kohno, Kim Laine, Shwetak Patel, and Franziska Roesner. 2023. Understanding people's concerns and attitudes toward smart cities. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–24.
[17] Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. Understanding Privacy Attitudes and Concerns Towards Remote Communications During the {COVID-19} Pandemic. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 695–714.
[18] Flavius Floare. 2024. Microsoft Teams could know if you're not paying attention during online meetings, according to new attention-tracking technology. Windows Report. https://windowsreport.com/microsoft-teams-could-know-if-youre-not-paying-attention-during-online-meetings-according-to-new-attention-tracking-technology/
[19] Nico Heitmann, Hendrik Siewert, Sven Moog, and Juraj Somorovsky. 2024. Security Analysis of BigBlueButton and eduMEET. In *International Conference on Applied Cryptography and Nebtwork Security*. Springer, 190–216.
[20] Muhammad Kamal Hossen and Mohammad Shorif Uddin. 2023. Attention monitoring of students during online classes using XGBoost classifier. *Computers and Education: Artificial Intelligence* 5 (2023), 100191.
[21] Dima Kagan, Galit Fuhrmann Alpert, and Michael Fire. 2023. Zooming into video conferencing privacy. *IEEE Transactions on Computational Social Systems* 11, 1 (2023), 933–944.
[22] Aaron Krolik and Natasha Singer. 2020. A feature on Zoom secretly displayed data from people's LinkedIn profiles. https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html.
[23] Annuri Praveen Kumar and N Siva Kumar. 2024. Zoom Classroom Engagement and Attention Detection System. In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*. IEEE, 1–6.
[24] Chen Ling, Utkucan Balcı, Jeremy Blackburn, and Gianluca Stringhini. 2021. A first look at zoombombing. In *2021 IEEE symposium on security and privacy (SP)*. IEEE, 1452–1467.
[25] Robertas Maleckas, Kenneth G Paterson, and Martin R Albrecht. 2023. Practically-exploitable Vulnerabilities in the Jitsi Video Conferencing System. *Cryptology ePrint Archive* (2023).
[26] Patrick E McKnight and Julius Najab. 2010. Mann-Whitney U Test. *The Corsini encyclopedia of psychology* (2010), 1–1.
[27] Carman Neustaedter, Saul Greenberg, and Michael Boyle. 2006. Blur filtration fails to preserve privacy for home-based video conferencing. *ACM Transactions on Computer-Human Interaction (TOCHI)* 13, 1 (2006), 1–36.
[28] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
[29] Justin Pot. 2024. The best video conferencing software for teams in 2025. https://zapier.com/blog/best-video-conferencing-apps/.
[30] 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 *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia*. 71–82.
[31] Prolific. retrieved December 2024. Prolific | Quickly find research participants you can trust. https://www.prolific.com.
[32] Qualtrics. retrieved December 2024. Qualtrics XM. https://www.qualtrics.com.
[33] Mohammad H Rajab and Mohammed Soheib. 2021. Privacy concerns over the use of webcams in online medical education during the COVID-19 pandemic. *Cureus* 13, 2 (2021).
[34] Reddit. 2020. Can anyone see who I pinned? https://www.reddit.com/r/Zoom/comments/fvvy3g/can_anyone_see_who_i_pinned/.
[35] Reddit. 2020. Disable video pinning. https://www.reddit.com/r/Zoom/comments/jommki/disable_video_pinning/.
[36] Reddit. 2020. Do people know if you pin their video? https://www.reddit.com/r/Zoom/comments/fvvb1x/do_people_know_if_you_pin_their_video/.
[37] Reddit. 2020. LPT: If you're using Zoom for work or school, be aware that Zoom has an attention tracking feature. https://www.reddit.com/r/LifeProTips/comments/fjtb9o/lpt_if_youre_using_zoom_for_work_or_school_be/.
[38] Reddit. 2020. Zoom desperately needs a feature to let you know when someone pins your video. https://www.reddit.com/r/Zoom/comments/jb1z3s/zoom_desperately_needs_a_feature_to_let_you_know/.
[39] Reddit. 2020. Zoom Hosts Can Easily See If You're Not Paying Attention and Automatically Track Attendance. https://www.reddit.com/r/YouShouldKnow/comments/g302ch/ysk_zoom_hosts_can_easily_see_if_youre_not_paying/.
[40] Reddit. 2020. Zoom: Pinning Videos? https://www.reddit.com/r/college/comments/j55gek/zoom_pinning_videos/.
[41] Reddit. 2021. May 23rd zoom participants will be required to consent to zoom recording disclaimers. https://www.reddit.com/r/Zoom/comments/nijr51/may_23rd_zoom_participants_will_be_required_to/.
[42] Reddit. 2024. How do you feel about recording every company meeting? https://www.reddit.com/r/WFH/comments/1am5mk6/how_do_you_feel_about_recording_every_company/.
[43] Reddit. 2024. Is there a way to hide yourself when you're being spotlighted during a meeting? https://www.reddit.com/r/Zoom/comments/15rlqex/is_there_a_way_to_hide_yourself_when_youre_being/.
[44] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.
[45] Tony Redmond. 2023. Teams adds explicit consent for recorded meetings. https://office365itpros.com/2023/03/13/explicit-consent-for-teams-recordings/.
[46] Thomas Reisinger, Isabel Wagner, and Eerke Albert Boiten. 2022. Security and privacy in unified communication. *ACM Computing Surveys (CSUR)* 55, 3 (2022), 1–36.
[47] Cedric Ryngaert and Mistale Taylor. 2020. The GDPR as global data protection regulation? (2020).
[48] Gwen Shaffer. 2021. Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy* 11 (2021), 222–265.
[49] Yogesh Shinde. 2024. Video conferencing market soar to USD 21 billion by 2032. https://scoop.market.us/video-conferencing-market-news/.
[50] Zoom Support. 2020. Attendee attention tracking. https://support.zoom.com/hc/ko/article?id=zm_kb&sysparm_article=KB0069153.
[51] Zoom Support. retrieved December 2024. Audio and video. https://support.zoom.com/hc/en/category?id=kb_category&kb_category=31293e9a8720391089a37408dabb35b8.
[52] Zoom Support. retrieved December 2024. Zoom meeting features. https://support.zoom.com/hc/en/category?id=kb_category&kb_category=42927a128720391089a37408dabb3572.
[53] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)*. 367–385.
[54] Sigal Tifferet. 2019. Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior* 93 (2019), 1–12.
[55] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, 3152676 (2017), 10–5555.
[56] Miranda Wei, Pardis Emami-Naeini, Franziska Roesner, and Tadayoshi Kohno. 2023. Skilled or Gullible*f* Gender Stereotypes Related to Computer Security and Privacy. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2050–2067.
[57] Lydia Weinberger, Christian Eichenmüller, and Zinaida Benenson. 2023. Interplay of Security, Privacy and Usability in Videoconferencing. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–10.
[58] Lydia Weinberger, Christian Eichenmüller, Freya Gassmann, Gaston Pugliese, and Zinaida Benenson. 2024. Used, Avoided, Restricted? Perceptions, Behavior, and Changes in Video Conferencing of German-speaking Users During and After the Pandemic. (2024).
[59] Robert F Woolson. 2005. Wilcoxon signed-rank test. *Encyclopedia of Biostatistics* 8 (2005).
[60] Elana Zeide and Helen Nissenbaum. 2018. Learner privacy in MOOCs and virtual education. *Theory and Research in Education* 16, 3 (2018), 280–307.

A Selection Process for Features of Interest

We selected four features stated in Section 3.1 based on the following process. In Table 2, we first list all features provided by Zoom [51, 52] excluding the accessibility features to better focus on the general features that are more widely used by the general public. We then filter the 124 features based on four criteria (i.e., generality, information flow, external control and increase in information sharing), applied sequentially. We stopped our analysis on a feature (thus, marking '-' in Table 2) whenever it is deemed unselected by any of the criteria. In Table 2, a feature is marked with 'o' if it satisfies the given criterion, with 'x' if it does not satisfy the given criterion, and with '–' if it was already considered unselected by another criterion:

(1) *Generality.* We excluded features that are not present in Google Meet and Microsoft Teams.
(2) *Information flow.* We retained only those that generate outbound information flow involving personal data.
(3) *External control.* Features were further selected only if they could be initiated or controlled by other participants.
(4) *Increase in information sharing.* The feature must either maintain or increase the amount of information shared about a participant.

For the feature classification task, two researchers independently classify each feature, then compare to each other to generate the final set.

After this process, we end up with five features marked highlighted in gray in Table 2. We then grouped the three features (i.e., managing computer recordings, using audio transcription for cloud recordings, and starting a cloud recording on iOS and Android) related to recording under a single *meeting recording* feature. Last, we added the attention tracking feature to the list. This feature satisfies all the criteria except the first one (i.e., generality); yet, we decided to make an exception and include it in our analysis because this feature used to be actively used in Zoom, is still provided by Webex [12, 13], and is planned to be introduced by Microsoft Teams [18]. After all the filtering processes, we ended up with the four features of interest: attention tracking, meeting recording, pinning and spotlighting.

B Demographics

We provide the participants demographics information and distribution of the information flow for each participants' group in Table 3.

C Transmission principles

The transmission principles are defined in Section 3.2.5, with a complete list for attention tracking presented in Table 1. The following section provides tables summarizing the transmission principles for additional features, including meeting recording (Table 4), pinning (Table 5), and spotlighting (Table 6).

D Survey Questionnaire

We provide the full survey questionnaire we used for the study. The survey is described in Section 3.3.

D.1 Screening Question (Section 3.3.1)

- For which purposes have you used video conferencing? (Select all that apply.)
  - Online lecture
  - Online discussion
  - Interview
  - Business meeting
  - Social gathering
  - Other

D.2 Feature Overview and Related-Question (Section 3.3.1)

Attention tracking. The attention tracking feature allows the host to monitor a participant's attention, by detecting when Zoom is not the active application on a participant's computer for more than 30 seconds during screen sharing. When a participant is detected to be inattentive, the attention tracker shows a clock icon next to the participants' name in the host's screen. At the end of each meeting, Zoom also generates a report listing the percentage of time each participant during the meeting.

- Have you heard of the attention tracking feature in Zoom?
  - No, I have never heard of attention tracking.
  - Yes, I have heard of attention tracking.

Meeting recording. In video conferencing platforms, the host can record the meeting using the recording feature. The recording includes all audio and visual information shown to the host, such as the video feeds and voices of the participants. Then, when the host starts to record, all participants receive a notification. After the meeting, the recorded data is stored in the host's local storage or in the cloud and can be used for various purposes.

- Did you know about the meeting recording feature in video conferencing platforms? Have you ever been at a meeting that was being recorded?
  - No, I did not know about meeting recording.
  - Yes, I knew about meeting recording, but I have never been at a meeting while recording.
  - Yes, I knew about meeting recording, and I have been at meetings while recording.

Pinning. In video conferencing platforms, pinning is a feature that allows you to bring a specific participant's video feed to your main screen, making it the primary video feed regardless of who is speaking. Pinning can be triggered by selecting the option from the dropdown menu, or simply by double-clicking on a participant's video feed.

- Did you know about the pinning feature in video conferencing platforms? Have you ever used it?
  - No, I did not know about pinning.
  - Yes, I knew about pinning, but I have never used it.
  - Yes, I knew about pinning, and I have used it.

Spotlighting. In video conferencing platforms, the host can spotlight a specific participant's video feed. The spotlighted participant is then set as the primary active speaker in the meeting, and all the other participants will see the spotlighted speaker.

- Did you know about the spotlighting feature in video conferencing? Have you ever been spotlighted?

- No, I did not know about spotlighting.
- Yes, I knew about spotlighting, but I have never been spotlighted.
- Yes, I knew about spotlighting, and I have been spotlighted.

D.3 Contextual Integrity Statements Questions (Section 3.3.2)

D.3.1 Baseline. The baseline questions are customized based on both the social context, recipient and the corresponding feature. In this section, we present templates for each feature. The *[social context]* and *[recipient]* placeholders in each statement are replaced with specific values, as detailed in Table 1 and Tables 4-6 in Appendix C.

Attention tracking. You are participating in a *[social context]* through a video conferencing platform. How acceptable is it for you when the following person tracks your attention during the *[social context]*?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[recipient]	○	○	○	○	○
[recipient]	○	○	○	○	○

Meeting recording. You are participating in a *[social context]* through video conferencing platforms. How acceptable is it for you when the following person records the meeting and your audio-visual data is included in the records?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[recipient]	○	○	○	○	○
[recipient]	○	○	○	○	○

Pinning. You are participating in a *business meeting* through a video conferencing platform, with your camera turned on. During the meeting, someone pins your video feed but you are unaware of who it is because the platform does not provide this information. How acceptable is it for you when the following person pins your video feed during the meeting?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[recipient]	○	○	○	○	○
[recipient]	○	○	○	○	○

Spotlighting. You are participating in a *[social context]* through a video conferencing platform. During the meeting, the host spotlights your video. How acceptable is it for you when your video is spotlighted and shown to everyone?

Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
○	○	○	○	○

D.3.2 Complete CI Statements. The complete CI questions are customized based on both the social context, feature, recipient and transmission principle. In this section, we present templates for each feature. The *[social context]*, *[recipient]*, and *[transmission principle]* placeholders in each statement are replaced with specific values, as detailed in Table 1 and Tables 4-6 in Appendix C.

Attention tracking. You are participating in a *[social context]* through a video conferencing platform. How acceptable is it for you when the *[recipient]* tracks your attention during the *[social context]* under the following conditions?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[*transmission principle*]	○	○	○	○	○
[*transmission principle*]	○	○	○	○	○

Meeting recording. You are participating in a *[social context]* through video conferencing platforms. How acceptable is it for you when *[recipient]* records the meeting and your audio-visual data is included in the recorded data under the following condition?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[*transmission principle*]	○	○	○	○	○
[*transmission principle*]	○	○	○	○	○

Pinning. You are participating in a *[social context]* through a video conferencing platform while turning on your camera. How acceptable is it for you when the *[recipient]* pins your video feed under the following condition?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[*transmission principle*]	○	○	○	○	○
[*transmission principle*]	○	○	○	○	○

Spotlighting. You are participating in a *[social context]* through a video conferencing platform. During the meeting, the host spotlights your video. How acceptable is it for you when your video is spotlighted and shown to everyone under the following conditions?

	Completely unacceptable	Unacceptable	Neutral	Acceptable	Completely acceptable
[*transmission principle*]	○	○	○	○	○
[*transmission principle*]	○	○	○	○	○

D.4 Demographics (Section 3.3.3)

- Please specify your gender.
  - Male
  - Female
  - Other
  - Prefer not to answer
- Please indicate your age.
  - _____

Table 2: Selection process for features of interest. The selected features are highlighted in gray.

Categories	Features	Generality	Information flow	External control	Increase in information sharing
Audio	Testing audio before Meetings	○	×	-	-
	Configuring audio for music and singing	×	-	-	-
	Using push-to-talk	○	○	×	-
	Using spatial audio in meeting and webinars	×	-	-	-
Video	Virtual background	○	○	×	-
	Using avatars	○	○	×	-
	Using blurred background	○	○	×	-
	Enhancing video	○	○	×	-
	Managing custom video filter	○	○	×	-
	Pinning participant's video	○	○	○	○
	Using focus mode	×	-	-	-
	Using immersive view	×	-	-	-
	Setting a custom gallery view order	×	-	-	-
	Stopping all incoming video	×	-	-	-
	Using far-end camera control	×	-	-	-
	Using meeting wallpaper	×	-	-	-
	Configuring auto-accept far-end camera	×	-	-	-
Recording	Managing computer recordings	○	○	○	○
	Using audio transcription for cloud recordings	○	○	○	○
	Adjusting recording video layouts	×	-	-	-
	Trimming cloud recordings	×	-	-	-
	Starting a cloud recording on iOS and Android	○	○	○	○
	Deleting computer or cloud recordings	○	×	-	-
	Starting recordings without the host	×	-	-	-
	Providing consent to be recorded	×	-	-	-
Screen sharing	Sharing your screen or desktop on Zoom	○	○	×	-
	Sharing background music or computer audio on Zoom	○	○	×	-
	Requesting or giving remote control	○	○	×	-
	Screen sharing a PowerPoint presentation	○	○	×	-
	Using annotation tools for collaboration	○	○	×	-
	Side-by-side mode for screen sharing	○	×	-	-
	Sharing a recorded video with sound during your meeting	○	○	×	-
	Sharing multiple screens simultaneously	×	-	-	-
	Sharing your screen while seeing all meeting participants	○	○	×	-
	Sharing a classic whiteboard	○	○	×	-
	Sharing your iOS screen from the Zoom mobile app	○	○	×	-
	Sharing your iOS screen from the Zoom desktop client	○	○	×	-
	Controlling slides shared by another participant	○	○	×	-
	Optimizing a shared video clip in full screen	×	-	-	-
	Sharing slides as a Virtual Background	×	-	-	-
	Adding an image watermark	×	-	-	-
	Screen sharing a Keynote presentation	○	○	×	-
	Following the presenter's pointer	×	-	-	-
	Using Screen Sharing Presenter layouts	×	-	-	-
	Using all screens mode in meetings	×	-	-	-
	Share an iOS device screen using a cable	×	-	-	-
	Collaborating on a document in a Zoom Meeting	○	○	×	-
Creating and scheduling meetings	Scheduling meetings	○	×	-	-
	Joining a Zoom test meeting	×	-	-	-
	Designating an alternative host	○	×	-	-
	Enabling and adding a co-host	○	×	-	-
	Scheduling and customizing a meeting with registration	○	×	-	-
	Scheduling a recurring meeting	○	×	-	-
	Using Personal Meeting ID (PMI)	×	-	-	-
	Using calendar and contacts integration	○	×	-	-
	Managing meeting and webinar registration	○	×	-	-
	Creating a permanent Zoom Meetings link	×	-	-	-
	Recovering a deleted meeting or webinar	○	×	-	-

	Where to find the meeting invitation text	○	×	-	-
	Converting meetings and webinars	×	-	-	-
	Creating personal meeting templates	×	-	-	-
	Making changes to a scheduled Zoom meeting	○	×	-	-
	Canceling a Zoom meeting	○	×	-	-
	Using public calendars with Zoom	○	×	-	-
	Importing meeting registrants by CSV upload	×	-	-	-
	Editing meeting details	○	×	-	-
	Rescheduling a meeting	○	×	-	-
	Scheduling a meeting from a template	×	-	-	-
Hosting meeting	Starting or joining a meeting as the host	○	×	-	-
	Understanding time limits for Zoom Meetings	○	×	-	-
	Customizing your personal meeting ID (PMI) and personal link	×	×	-	-
	Using waiting room	○	×	-	-
	Using host and co-host controls in a meeting	○	×	-	-
	Hosting multiple meetings simultaneously	○	×	-	-
	Understanding meeting participant limits	○	×	-	-
	Muting/unmuting request participants in a meeting	○	×	-	-
	Spotlighting participants' videos	○	○	○	○
	Managing participants in a meeting	○	×	-	-
	Viewing participant attendance status in a meeting	○	○	×	-
	Changing security settings in a Zoom meeting	○	×	-	-
	Passing host controls to leave the meeting	○	×	-	-
	Signing in and claiming host during a meeting	×	-	-	-
	Using Remote support session	×	-	-	-
	Reporting inappropriate behavior	○	○	×	-
	Restricting meeting capacity	○	×	-	-
Participating in meeting	Joining a Zoom meeting without an account	○	×	-	-
	Joining a meeting with the invite link	○	×	-	-
	Using gesture recognition	○	○	×	-
	Hot keys and keyboard shortcuts	○	×	-	-
	Starting a meeting without the host present	○	×	-	-
	Showing and hiding your video in a meeting	○	○	×	-
	Participant controls in a meeting	○	×	-	-
	Muting/unmuting yourself during a Zoom meeting	○	○	×	-
	Waiting for the host to start meeting/webinar	○	×	-	-
	Sending a file in meetings and webinars	○	○	×	
	Joining a Zoom meeting anonymously	×	-	-	-
	Using Zoom for Tesla	×	-	-	-
	See My Video	○	×	-	-
	Profile cards in Zoom Meetings and Team Chat	×	-	-	-
	Hide My Video	○	×	-	-
	Using Zoom on a foldable device	○	×	-	-
	Declining a meeting invite with a message	○	×	-	-
	Zoom's Terms of Service update notifications	×	-	-	-
	Taking the end-of-meeting experience feedback survey	×	-	-	-
	Active App Notifier	×	-	-	-
Participant engagement feature	Creating and using continuous meeting chat	○	×	-	-
	Conducting polls in meetings	○	×	-	-
	Managing meeting breakout rooms	○	×	-	-
	Pre-assigning meeting participants to breakout rooms	○	×		-
	Conducting quizzes in meetings	×	-	-	-
	Chatting in a Zoom meeting	○	○	×	-
	Participating in meeting breakout rooms	○	×	-	-
	Using post-meeting survey and reporting	×	-	-	-
	Sharing screen and broadcasting to breakout rooms	×	-	-	-
	Managing Zoom Surveys as user	×	-	-	-
	Using the new meeting chat experience	×	-	-	-
	Creating meeting breakout rooms from poll results	×	-	-	-
	Assigning polls and quizzes to specific meetings or webinars	×	-		-
Livestreaming capability	Live streaming meetings or webinars on Facebook	×	-	-	-

	Livestreaming meetings or webinars on YouTube	×	-	-	-
	Livestreaming meetings or webinars on a custom site	×	-	-	-
	Adding a live streaming watermark	×	-	-	-
	Livestreaming meetings or webinars on Workplace	×	-	-	-
	Livestreaming meetings or webinars on Twitch	×	-	-	-

		Gender distribution			Age				Distribution of information flows		
Group	Total	Male	Female	Self-described	Avg.	Med.	Min.	Max.	Social Context	Feature (Recipient)	Number of information flows
1	118	57	58	3	36.96	35	18	79	Business meeting	Attention tracking, Spotlighting	29
2	113	58	53	2	37.80	35	20	66		Meeting recording (Leadership, External partner)	35
3	111	50	58	3	38.37	35	18	73		Meeting recording (Team member), Pinning	35
4	109	53	53	3	32.40	31	18	69	Online lecture	Attention tracking, Spotlighting	28
5	112	62	49	1	31.73	30	18	73		Meeting recording	30
6	101	50	45	5	33.03	29.5	19	64		Pinning	35
7	105	55	47	3	36.10	36	18	64	Social gathering	Meeting recording, Pinning, Spotlighting	26
Total	769	385	364	20	35.25	33	18	79			

Table 3: Demographics of the participants and the distribution of information flows per group. A total of 769 participants were divided into seven groups based on social contexts, features, and recipients.

			Social Contexts and Recipients					
			Business meeting			Online lecture		Social Gathering
			Leadership (e.g., boss)	Team member	External partner	Instructor	Teaching Assistant	Friend
Categories from GDPR and Transmission Principles	Consent	Explicit consent required	If you have given explicit consent about being recorded and approved it					
	Storing period	Data stored short period	If the recorded data is destroyed after a short period of time					
		Storage duration unknown	If it's unknown for how long the recorded data is stored					
	Control personal information	Audio not recorded	If the recorded data includes only your video but not your audio					
		Video not recorded	If the recorded data includes only your audio but not your video					
		Video blurred	If your video is blurred					
		Voice modulated	If your audio is adjusted through voice modulation					
	Notification of data usage	No notification given	If there is no notification when your are being recorded					
	Data sharing	Shared publicly	If the recorded data is shared publicly					
		Shared privately	If the recorded data is shared within your team			If the recorded data is shared with students in the same lecture		If recorded data is shared with friends
	Purpose of data usage	Used for meeting review	If the recorded data is used for reviewing the content of meeting			If the recorded data is used for reviewing the lecture		n/a
		Used for evaluation	If the recorded data is used for evaluating your performance	n/a	n/a	If the recorded data is used for checking attendance		n/a
		Used for profiling	If the recorded data is used for identifying specific characteristics of employees, such as their reactions to the lecture, to enhance future lectures	n/a	n/a	If the recorded data is used for identifying specific characteristics of students, such as their reactions to the lecture, to enhance future lectures		n/a
		Used for fun	n/a	To capture your audio-visual data for fun		n/a		n/a
		Used for AI training	If the recorded data is used for training AI models					n/a
	Anonymization	Data anonymized	If your name is redacted from the recording					

Table 4: Table of transmission principles for meeting recording. We enumerate transmission principles based on social contexts, recipients, and GDPR principles.

			Social Contexts and Recipients								
			Business meeting			Online lecture					Social gathering
			Leadership (e.g., boss)	Team member	External partner	Instructor	Teaching assistant	Friend	Acquaintance	Stranger	Friend
Categories from GDPR and Transmission Principles	Consent	Explicit consent required	If there is an option for you to enable/disable pinning your video feed from all participants, and you decide to enable it								
	Control personal information	Option to control feed size	If there is an option to limit the maximum tile size of how your video feed is displayed on others' screen								
		Option to control pinning time limit	If there is an option to limit the time other participants can pin you								
	Notification of data usage	Receive notification when pinned	If you receive a notification and thus learn who is pinning you, and the *[recipient]* who pins you is aware of this notification								
	Purpose of data usage	Pinned while speaking	If you are pinned while you are actively speaking with your microphone turned on								
		Pinned while muted	If you are pinned while you are muted and not speaking								
	Forced to turn on camera	Forced to turn on camera	If you are forced to turn on the camera								

Table 5: Table of transmission principles for pinning. We enumerate transmission principles based on social contexts, recipients, and GDPR principles.

			Social Contexts and Recipients		
			Business meeting	Online lecture	Social gathering
			Everyone		
Categories from GDPR and Transmission Principles	Consent	Explicit consent required	If you have given explicit consent for your video feed to be spotlighted by the host and approved it		
	Control personal information	Option to control feed size	If there is an option to limit the maximum tile size of how your video feed is displayed on others' screen		
		Option to control spotlight time limit	If there is an option to limit the time other participants can pin you		
		Can remove spotlight	If you can remove (i.e., disable) the spotlight after the host spotlights your video		
	Purpose of data usage	Spotlighted while speaking	If you are spotlighted while you are actively speaking with your microphone turned on		
		spotlighted while muted	If you are spotlighted while you are muted and not speaking		
	Anonymization	Data anonymized	If the spotlighted video is anonymized (i.e., no name on your spotlighted video)		
	Situational context	Participant compositions	If the most participants are supervisors	If majority of participants of the lecture are of opposite sex	If majority of participants are acquaintances rather than close friends
			If the most participants are external partners		

Table 6: Table of transmission principles for spotlighting. We enumerate transmission principles based on social contexts, recipients, and GDPR principles.

E Additional Figures

We provide the additional figures that we complement in Section 4.3 and Section 4.4.

E.1 Figures of transmission principles

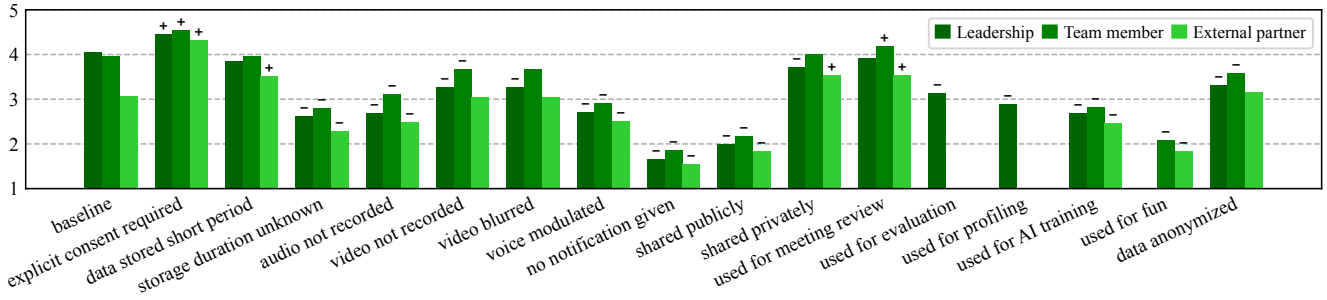
We provide the average acceptability scores of transmission principles for meeting recording, pinning and spotlighting feature in Figure 7; see Section 4.3 for detailed information.

E.2 Gender

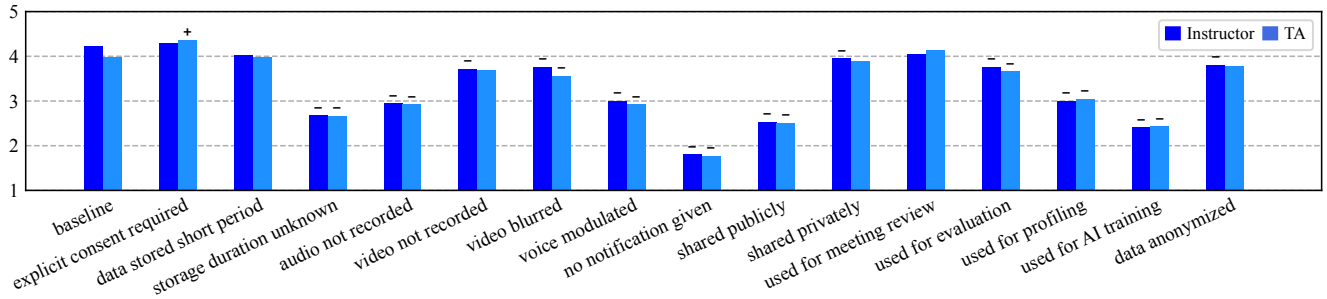
Detailed information on gender differences for the meeting recording feature is provided in Figure 3 in Section 4.4.1. Since the findings are similar, we provide the figure of pinning here; see Figure 9. Attention tracking (Figure 8) and spotlighting (Figure 10) show minimal gender differences; therefore, we did not delve further into these features.

E.3 Prior Experience

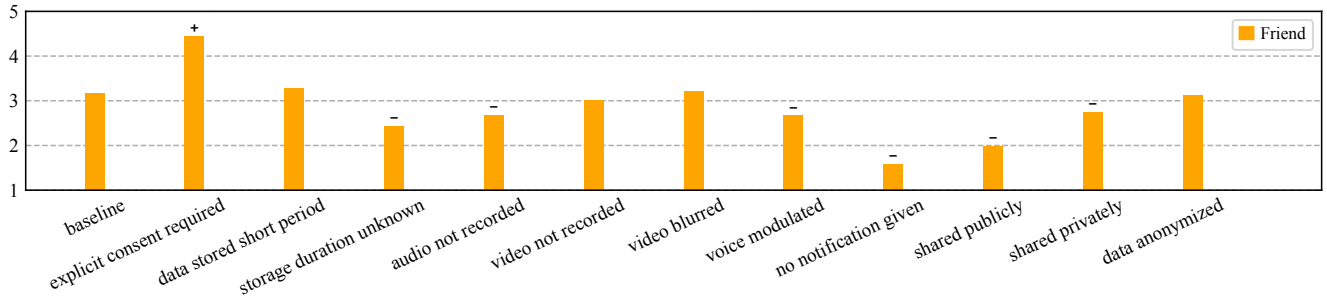
Detailed information regarding the pinning feature is available in Figure 4 in Section 4.4.2. Since the findings are similar, we provide the result of spotlighting here; see Figure 13. The majority of participants answered that they had not known about the attention tracking feature (Figure 11) and had experienced meeting recording (Figure 12). Due to the imbalance, it is hard to clearly identify the difference between two groups. Nevertheless, the general trend remains: participants with prior experience show higher acceptability toward the feature.



(a) Business meeting



(b) Online lecture



(c) Social gathering

Figure 5: Average acceptability scores for the meeting recording feature on baseline and transmission principle conditions, across different recipients in social contexts of (a) business meeting, (b) online lecture, and (c) social gathering. The '+' or '−' marks indicate the statistical significance of $p < 0.05$, where '+' and '−'indicate the acceptability score being higher and lower than the baseline, respectively.

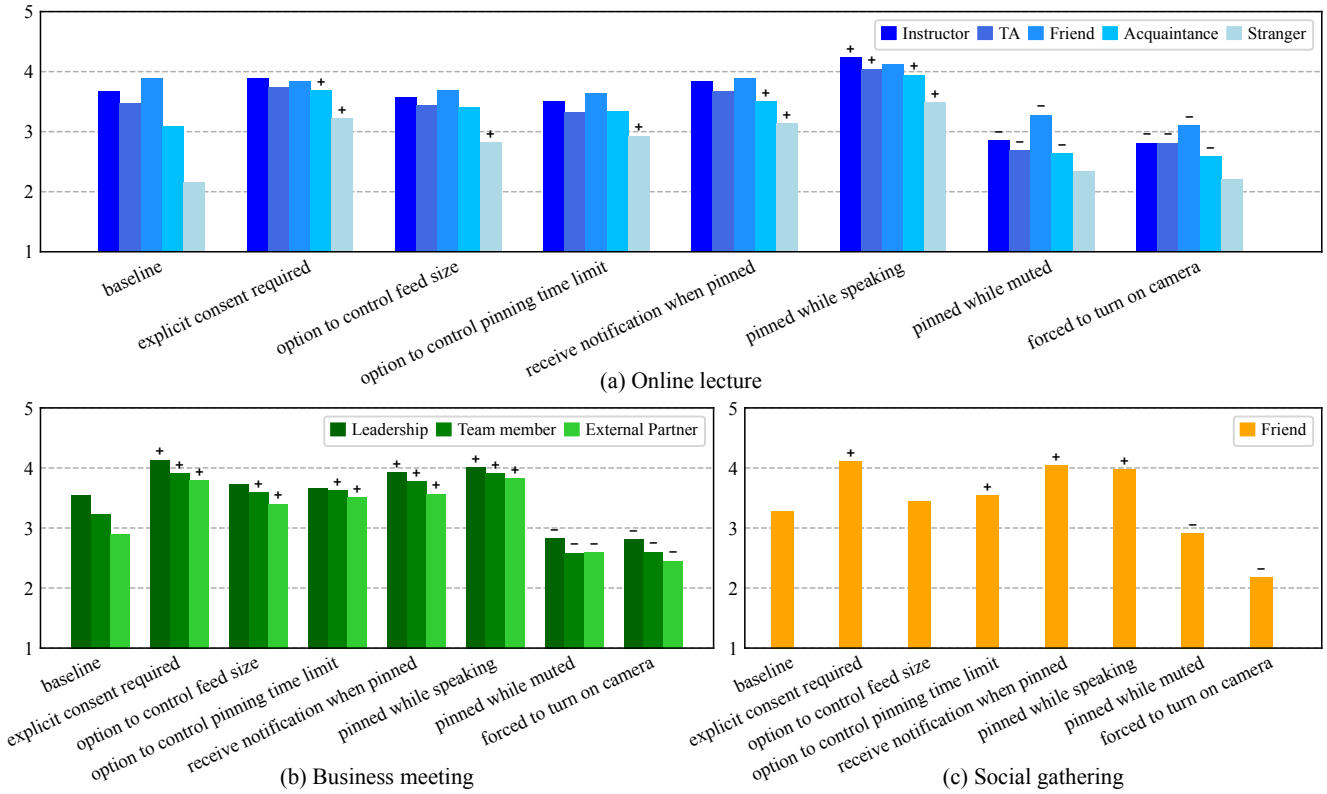


Figure 6: Average acceptability scores for the pinning feature on baseline and transmission principle conditions, across different recipients in social contexts of (a) online lecture, (b) business meeting, and (c) social gathering. The '+' or '−' marks indicate the statistical significance of $p < 0.05$, where '+' and '−' indicates the acceptability score being higher and lower than the baseline, respectively.

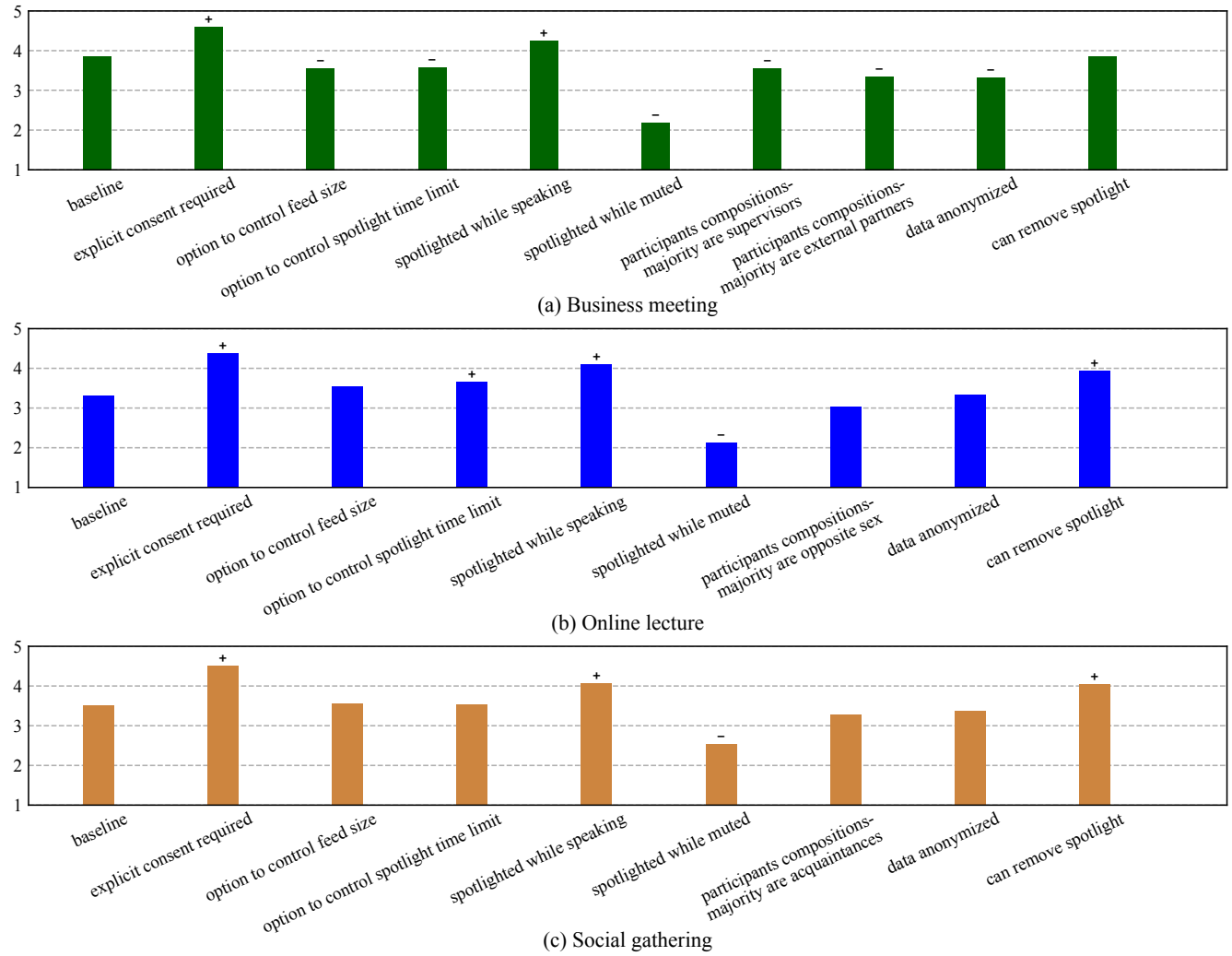


Figure 7: Average acceptability scores for the spotlighting feature on baseline and transmission principle conditions in social contexts of (a) business meeting, (b) online lecture, and (c) social gathering. The '+' and '–' marks indicate the statistical significance of $p < 0.05$, where '+' and '–' indicates the acceptability score being higher and lower than the baseline, respectively.

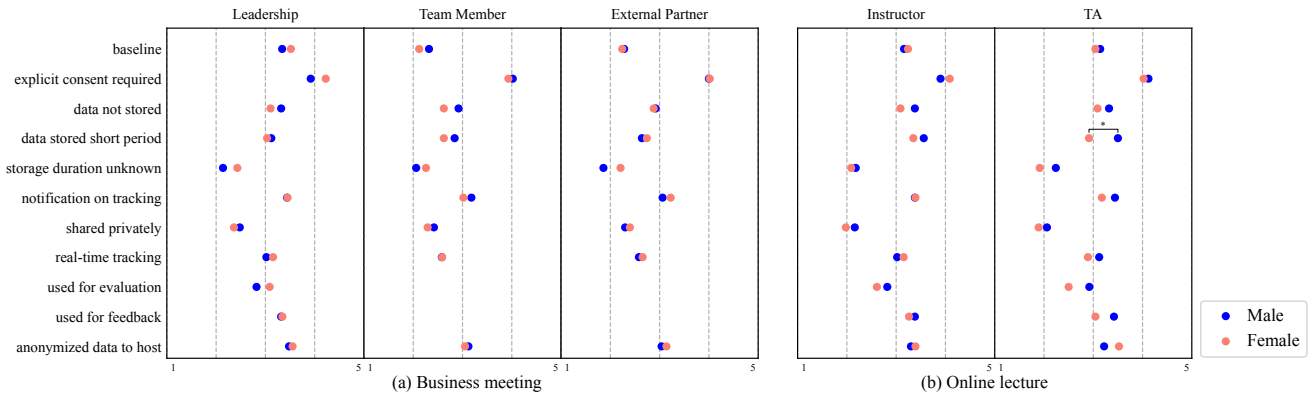


Figure 8: Average acceptability scores for the attention tracking feature by gender groups, across various transmission principles and recipient types, in the social contexts of (a) business meeting and (b) online lecture. (*) indicates statistical significance, with $p < 0.05$

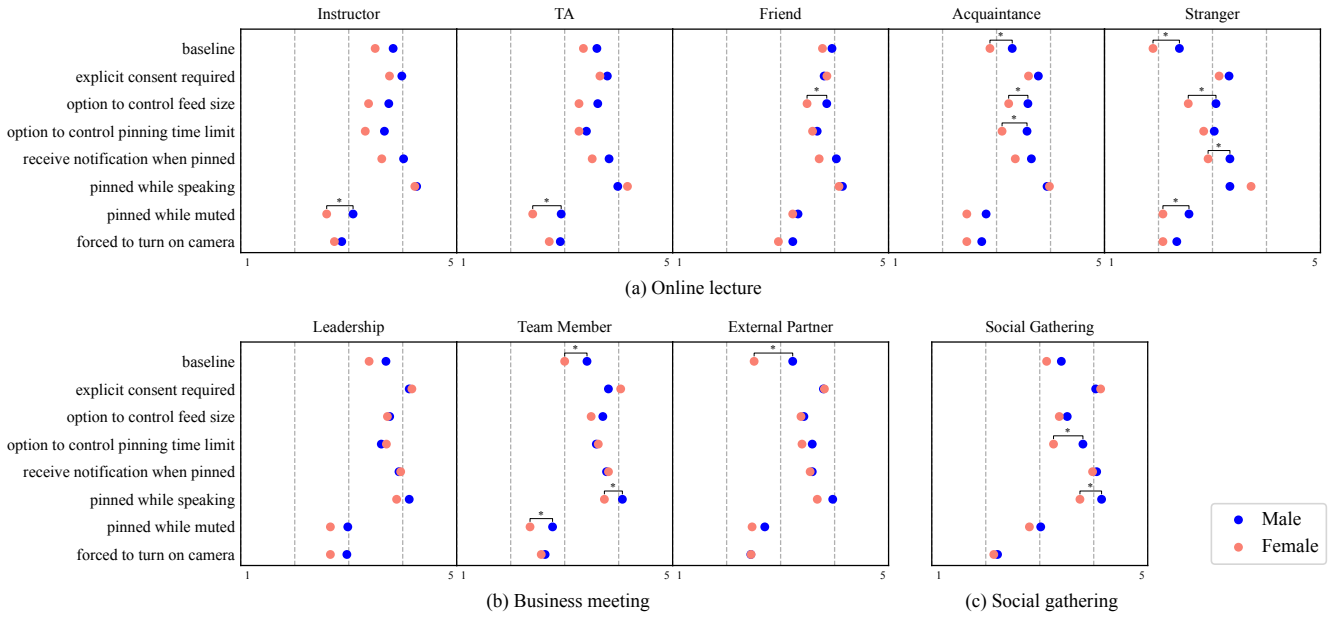


Figure 9: Average acceptability scores for the pinning feature by gender groups, for the given transmission principle (left) and recipient type (top), in the social context of (a) online lecture, (b) business meeting, and (c) social gathering. (*) indicates statistical significance, with $p < 0.05$.

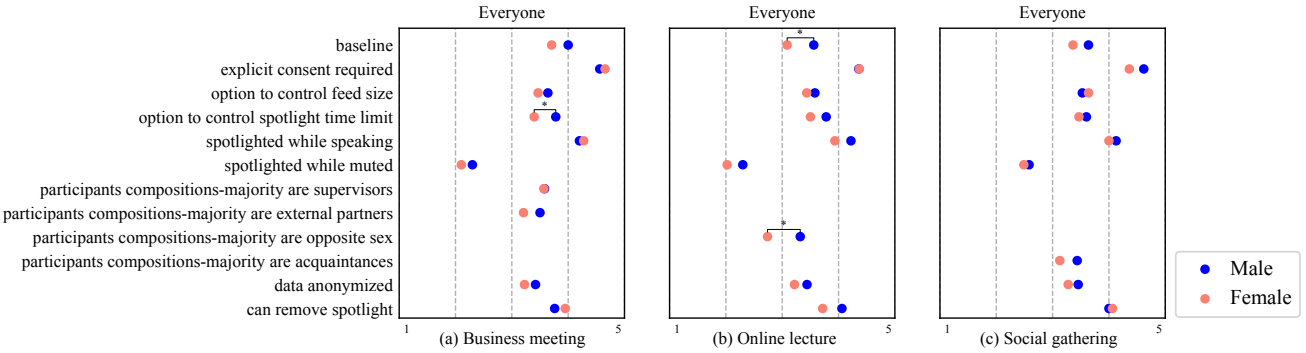


Figure 10: Average acceptability scores for the spotlighting feature by gender groups, across various transmission principles and recipient types, in the social contexts of (a) business meeting, (b) online lecture, and (c) social gathering. (*) indicates statistical significance, with p < 0.05.

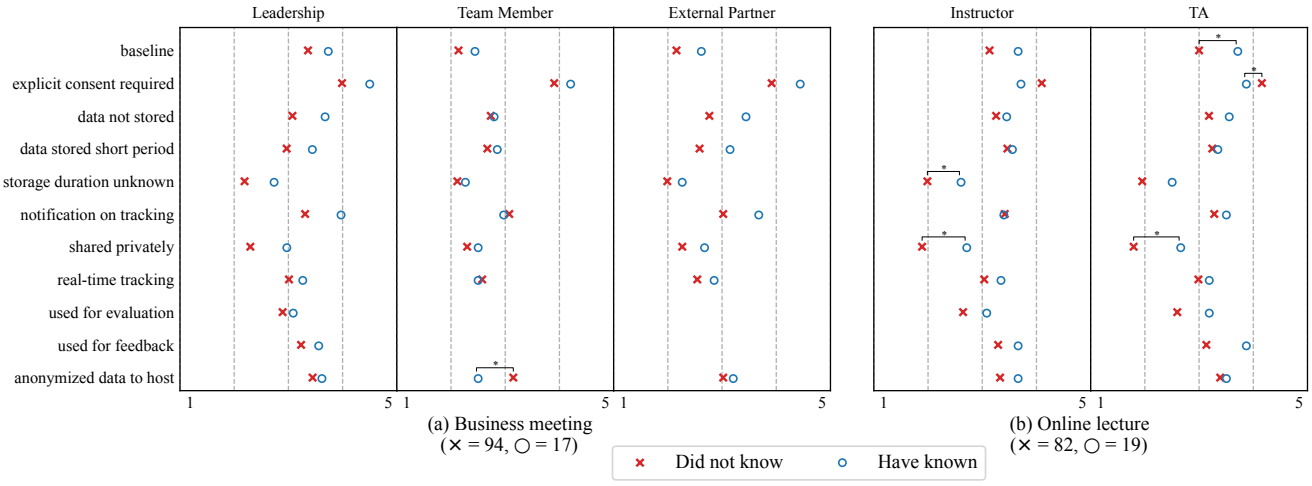


Figure 11: Average acceptability scores for the attention tracking feature by participants with different prior experiences, for the given transmission principle (left) and recipient type (top), in the social contexts of (a) business meeting and (b) online lecture. Parentheses indicate the number of participants in each group. (*) indicates statistical significance, with p < 0.05.

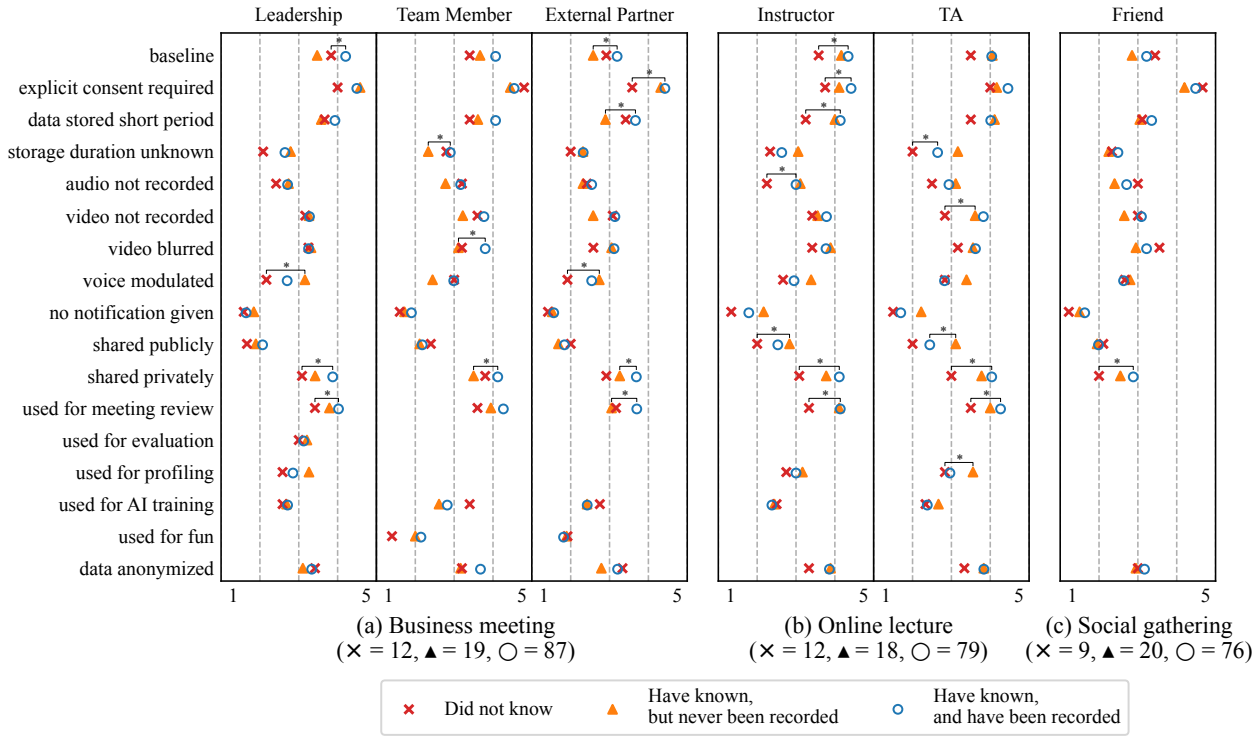


Figure 12: Average acceptability scores for the meeting recording feature by participants with different prior experiences, for the given transmission principle (left) and recipient type (top), in the social contexts of (a) business meeting, (b) online lecture, and (c) social gathering. Parentheses indicate the number of participants in each group. (*) indicates statistical significance, with $p < 0.05$.

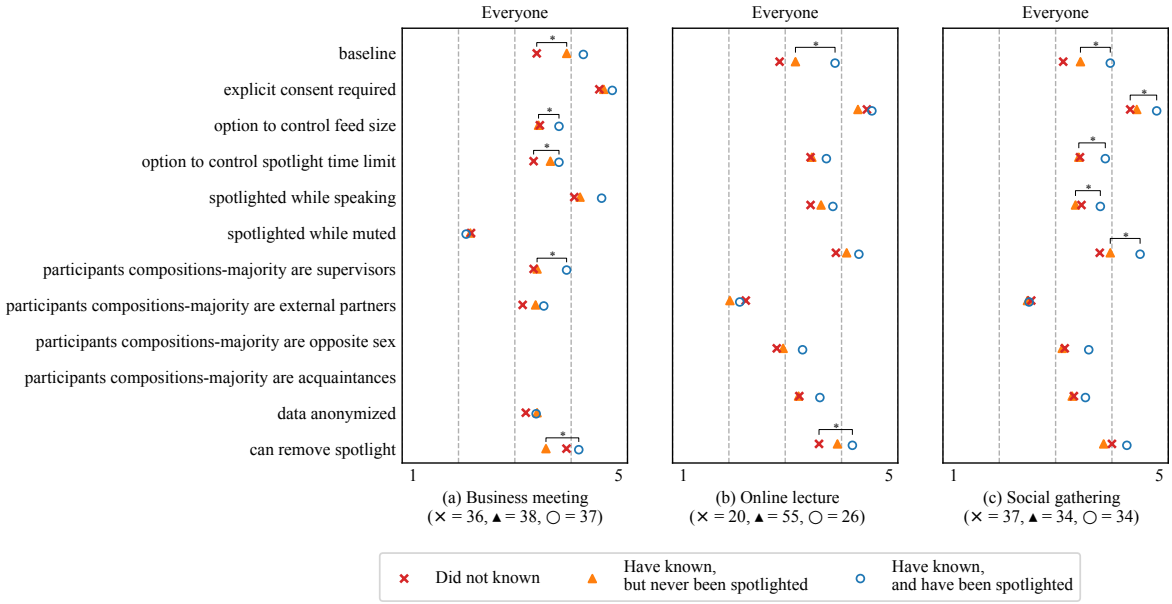


Figure 13: Average acceptability scores for the spotlighting feature by participants with different prior experiences, for the given transmission principle (left) and recipient type (top), in the social contexts of (a) business meeting, (b) online lecture, and (c) social gathering. Parentheses indicate the number of participants in each group. (*) indicates statistical significance, with $p < 0.05$.