Designing the Informing Process with Streamers and Bystanders in Live Streaming

Yanlai Wu, *University of Central Florida;* Xinning Gui, *The Pennsylvania State University;* Yuhan Luo, *City University of Hong Kong;* Yao Li, *University of Central Florida*

https://www.usenix.org/conference/soups2024/presentation/wu

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Designing the Informing Process with Streamers and Bystanders in Live Streaming

Yanlai Wu
University of Central Florida

Xinning Gui
The Pennsylvania State University

Yuhan Luo
City University of Hong Kong

Yao Li
University of Central Florida

Abstract

The ubiquity of synchronous information disclosure technologies (e.g., live streaming) has heightened the risk of bystanders being unknowingly captured. While prior work has largely focused on solutions aimed only at informing the key stakeholder - bystanders, there remains a gap in understanding how device owners and bystanders mutually expect the informing process, which is critical to ensure successful informing. To address this gap, we utilized live streaming as a case study and conducted a design ideation study with 21 participants, including both streamers and bystanders. Our focus was to understand streamers' and bystanders' needs for informing regarding bystander privacy at the ideation state and derive design principles. Participants' design ideas reflected various and nuanced privacy concerns, from which we identified key design principles for future design.

1 Introduction

Synchronous information disclosure, where the creation and consumption of information occur simultaneously in the same space [19, 65], has surged in recent years. Live streaming, a popular example of this technology, facilitates real-time self-presentation, experience sharing, and interaction among users, exemplifying synchronous broadcasting [19, 59, 65]. Despite the benefits of immediate information sharing, synchronous information disclosure poses significant privacy risks to bystanders, who are inadvertently captured in device owners' information sharing [13, 15]. Bystanders, ranging from passersby to close contacts such as roommates and family members, often find themselves unexpectedly exposed, with limited control over the personal information they wish to keep private. The broad spectrum of personal data collected in synchronous information disclosure, including visual and auditory information, exacerbates the risks of exposure [5,46,64], thereby elevating privacy concerns [16,31,38]. Prior research and news have reported bystanders were worried about their personal information [28, 58] being captured [11,53], stalked [67], and misinterpreted [16,58], leading to a series of negative consequences for them, such as financial loss [41], negative reputation [54], and harassment [7].

Prior research underscores the critical role of informing as a fundamental privacy protection for bystanders [2, 35, 60]. Informing here typically refers to enabling bystanders to be aware of the data sharing practices, the use of their personal information and the potential privacy risks [66]. Discussions have centered on enabling device owners to notify bystanders about their inclusion in information sharing activities [10,28]. As the devices used for synchronous information disclosure like cameras and microphones become more integrated into everyday items like smartphones and wearables, it becomes increasingly difficult for bystanders to recognize when they are being recorded [2, 64]. Consequently, researchers have designed indicators [1, 2, 12, 16, 60], notifications [37, 46, 60, 68], and alerts [26, 52] to improve bystanders' awareness of potential privacy invasions. Yet, these solutions have largely designed based on the bystanders' perspective [1, 2, 37, 46, 60, 68], leaving the perceptions, concerns and challenges of device owners in the informing process largely unexamined.

On the other hand, the informing process should not be viewed as unidirectional (from device owners to bystanders only). Bystanders might also need to communicate their privacy preferences to device owners to ensure their privacy expectations are met. While this dynamic has been explored in the context of asynchronous information disclosure, such as allowing bystanders to express their consent and concerns to the photo owners [3, 55, 68], it has received less attention in synchronous settings. The instantaneous nature of synchronous information disclosure offers limited opportunity for bystanders to convey their preferences before being captured, raising questions about the mechanisms through which bystanders prefer to inform of their concerns and how device owners interpret and act upon such feedback.

Therefore, there exists a notable gap in research on reciprocal informing practices between device owners and bystanders. Several crucial questions remain unanswered: Do device owners intend to inform bystanders about their potential inclusion? Do bystanders wish to communicate their privacy preferences to device owners? How do both parties view the informing process? What obstacles might they encounter while attempting to inform each other? To address these questions, it is essential to explore the mutual expectations of device owners and bystanders regarding informing.

Our study aims to fill this gap through a case study of live streaming. We chose live streaming for three reasons. First, live streaming is an increasingly popular form of real-time social media and it easily involves bystanders in various settings, such as private spaces, public areas, and online [16, 29, 30, 64]. Second, different from other synchronous devices such as IoT and AR, live streaming is more interpersonal as it allows direct and synchronous information disclosure to large anonymous viewers, which poses greater challenges for bystanders. Third, streamers, who are the device owners, aim to create content to attract a broad audience and earn profit [65], thus may weigh their own interests over bystander privacy. With live streaming as the study site, we seek to answer the following research questions:

RQ1: What needs, challenges and constraints of informing do streamers and bystanders have when it comes to bystander privacy in live streaming?

RQ2: What design do streamers and bystanders envision to address these needs, challenges and constraints?

To address these research questions, we engaged 21 participants with both streamers and bystanders in live streaming to conduct a design ideation study [22]. Design ideation involves generating, refining, and communicating ideas [25]. This process often marks the beginning of an imaginative and inventive approach [61]. In this paper, we used design ideation as a way to examine streamers and bystanders' various and nuanced design ideas that reveal both bystanders' and streamers' privacy needs for informing related to bystander privacy across streaming scenarios. Based on the ideas proposed by the participants and the design rationale for each idea, we derived design principles for the informing process that address bystander privacy.

The contributions of our paper are three-fold. First, we advance the understanding of bystander privacy by exploring the informing process from a multi-stakeholder perspective. Second, our findings reveal the multifaceted, nuanced, intricate, and dynamic nature of collective privacy management in the context of interpersonal and synchronized content-sharing platforms. Third, we propose key design principles for the informing through user-centric design, guiding the design of future synchronous information disclosure technologies.

2 Related Work on Informing Mechanisms for Bystander Privacy Protection

Extensive research has explored the privacy vulnerability of unaware bystanders in diverse socio-technical contexts [2, 4, 16, 21]. These contexts involve both asynchronous and synchronous information disclosure. As bystander privacy was initially noted in asynchronous information disclosure (e.g, photo sharing) and then intensified with the proliferation of technologies in synchronous information disclosure (e.g., live streaming), we first review prior work regarding informing mechanisms in asynchronous information disclosure and next move to synchronous information disclosure.

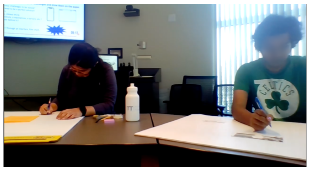


Figure 1: Two participants are designing in a design ideation study session

2.1 Informing in Asynchronous Information Disclosure

In asynchronous information disclosure, users' content production and consumption do not happen at the same time and space [65]. Examples of asynchronous information disclosure are social media posts, instant messaging, discussion forums, and so on. In these contexts, users generate content that can be reviewed, edited, or withdrawn before being received by the recipients. Regarding bystander privacy in asynchronous information disclosure, most research attention is on collaborative photo sharing [10, 27, 34, 63]. Bystanders, who are pictured, mentioned, linked or tagged other than the photo owners who share the picture [10, 18], are often unaware of being featured in others' photo sharing [34, 68]. Bystanders in collaborative photo sharing lack control over their personal information, as photo owners decide how and with whom the images are shared [23, 24]. As such, bystanders often worry about appearing inappropriately, such as being captured as drunk or undressed in group photos on social media [28].

Researchers have proposed diverse informing solutions. Earlier research has focused on informing bystanders of bystanders' involvement [20]. Xu et al. [66] propose a face-recognition algorithm to identify and inform bystanders about potential privacy violations. More recent research shifts towards a more interactive approach, highlighting the necessity of obtaining consent from bystanders and facilitating negotiation between both two parties. For example, Facebook enables tagged bystanders to ask the photo owners to limit the visibility of their tagged photo [6]. Zheng et al. [68] propose an access-control protocol that mandates the consent of all parties in a photo before sharing it. Salehzadeh et al. [42] suggest a mediator to remind the photo owner to obtain consent from bystanders, and use middle-ground solutions to support conflict-solving [55]. Mosca & Such [40] present a multi-step negotiation agent to discuss the sharing policy between both parties, considering their sharing preferences and moral values. Nourmohammadzadeh et al. [44] introduce a multi-agent system where an algorithm calculates user opinions based on user personality and behavior. However, the design solutions for asynchronous information disclosure may not apply to synchronous contexts where bystanders' data is collected in real-time, constantly, and goes beyond images.

2.2 Informing in Synchronous Information Disclosure

In synchronous information disclosure, users generate and consume information simultaneously [19, 65], such as IoT devices (e.g., smart home devices), wearable cameras, AR, and live streaming. Different from asynchronous information sharing, these technologies are normally less visible [1, 2, 64], operate continuously, and immediately capture a larger set of bystanders' personal information, such as bystanders' images, voices and movements [29, 37]. Due to this real-time, always-on, and continuous nature, it is more challenging for bystanders to be aware of being recorded in synchronous information disclosure than asynchronous information disclosure. This leads to bystander privacy concerns such as unknowingly being recorded saying inappropriate words [37], performing sensitive activities (e.g. withdrawing money on ATM) [53], or going to private locations [14].

To inform bystanders of their involvement in synchronous information disclosure, researchers have focused on design solutions across different technologies. In IoT, researchers aim to inform bystanders by enhancing the visibility and physical interaction with these devices. For example, Ahmad et al. [2] suggest that IoT devices should be designed to clearly display their sensor activities, such as showing on/off states to bystanders. Thakkar et al. [60] propose a bystander mode in mobile apps, enabling bystanders to view data relevant to themselves. Marky et al. [37] found that bystanders prefer various informing methods, including verbal communication, signs, notifications, and social media alerts. Pierce et al. [52] propose a mobile app that alerts bystanders about nearby smart cameras or microphones.

Prior work also indicates bystanders not only want to be informed but also want to have the option to control the IoT devices, which can offer them a sense of security [36, 49]. For example, Park et al. [49] propose different modes of control for bystanders in IoT. Bystanders in Marky et al.'s work express a desire to erase and block any data gathered about them by smart home devices [38]. Mare et al. [36] propose an interactive dashboard in smart home devices for Airbnb guests to access important details about and control the home's devices. Similar to this, Pierce et al. [52] introduce a guest account feature that allows bystanders limited access to IoT devices.

Besides IoT, for wearable devices, Perez et al. [50] developed FacePET, a wearable system for bystanders to manage privacy against unauthorized facial recognition. In AR, studies about informing are focused on informing AR users of the presence of bystanders to avoid interrupting the AR user's experience, rather than protecting the privacy of the bystanders [39, 45, 47].

In live streaming, to our best knowledge, only one study by Faklaris et al. [16] has proposed ways to inform bystanders in public and semi-public spaces, such as using colored lights on smartphones to signal active streaming and a 'Do Not Record' facial recognition database to blur registered faces. While [16] examines bystander attitudes toward being streamed in outdoor settings solely from the bystander's perspective, the informing process in live streaming involves multiple stakeholders, including both streamers and bystanders [64], the challenges and the designs envisioned in informing for multiple stakeholders remain unaddressed.

In sum, previous research related to synchronous information disclosure explores the informing process from the perspective of a single stakeholder, mostly the bystanders. Although Thakkar et al. [60]'s study includes both IoT device owners and bystanders, they examine each stakeholder's individual privacy needs rather than their mutual understanding of bystander privacy. However, bystander privacy protection requires mutual effort between the device owners and bystanders. As per communication privacy management (CPM) [51], all stakeholders need to negotiate and agree on their privacy expectations to ensure mutual privacy protection. While bystander is the key, the exclusion of device owners raises uncertainties about device owners' considerations in this matter. Therefore, it is crucial to design informing from a multi-stakeholder perspective.

Additionally, prior work focuses on synchronous technical platforms where bystander data are received by device owners or service providers to promote convenience [43] and automation [48]. However, with the rise of synchronous social platforms such as live streaming, information disclosure has become more interpersonal and involves social aspects such as self-presentation [65], relationship building [57], and interaction enhancement [9]. Thus, it is essential to integrate the interpersonal nature into the informing solutions.

To fill these gaps, we choose live streaming as a case study to explore the informing process about bystander privacy with bystanders and streamers. We conduct a design ideation study to delve into the multi-stakeholder perspectives and considerations, which will be debriefed next.

3 Methods

3.1 Participants & Recruitment

We conducted design ideation sessions (Figure 1) in April 2023 with a total of 21 participants, including 3 participants who identified themselves as streamers only, 8 as bystanders only, and 10 as both streamers and bystanders. This diverse group was recruited to provide various viewpoints and develop comprehensive design solutions to address bystanders' privacy in live streaming. Our study was approved by the university IRB.

Our study's participants consisted of 14 males and 7 females, with ages ranging from 18 to 45 years old. Recruitment was conducted through various channels, including word-of-mouth, flyers, university mailing lists, and social media platforms (Facebook, Twitter, and Reddit). Participants who were interested in our study were first asked to complete an online screening survey. This survey included a consent sheet and questions regarding their demographics, how they want to participate in the research (in person or via Zoom), their email addresses, their role as a streamer and/or a bystander, and their experience with live streaming or being live streamed. Participants who are under 18 years old and have no experience as a streamer or bystander are excluded. The demographic information of participants is presented in Table B in Appendix.

According to participants' preferences and availability, we organized 3 online design ideation sessions through Zoom with an average of 2 participants per session, and 10 in-person design ideation sessions, with an average of 1 to 5 participants per session. While we aimed to have at least two participants in each session to foster diverse perspectives and collaborative brainstorming, some were unable to attend due to personal reasons, resulting in some solo sessions. To ensure a diverse range of perspectives, we strategically grouped participants in various combinations: bystanders only, streamers only, and bystander with streamer. To minimize potential biases, we ensured that participants who were acquainted with each other were assigned to different groups. Two researchers participated in the design ideation sessions. Each session took about 2 hours, and each participant was compensated with $40 in cash at the end of the study.

3.2 Design Ideation Sessions

Each session began with a warm-up activity, followed by a design ideation activity, and concluded with a debriefing interview. The primary goal of these sessions was to explore potential informing mechanisms to address bystander privacy concerns in live streaming.

Warm-up Activity Each session began with a round-table introduction. We then asked each participant to jot down 1-3 privacy challenges that bystanders would encounter in live streaming on a card. For online participants, they were asked to write down the challenges on their own papers. We displayed a slide to guide their thoughts. In the slide, we first explained who are considered bystanders in live streaming, including unknown passersby in public spaces, known people in the household (e.g., family, friends, and roommates), and virtual bystanders (e.g., in-game teammates and contacts in an online conversation). We then listed a set of questions, such as what personal information of bystanders was streamed, any consequences, and where the disclosure happened. To avoid potential biases, we rephrased privacy in terms of personal information that bystanders do not want to share with the audience. Bystanders could draw from their own experiences, while streamers were encouraged to consider potential challenges their bystanders might face or as if they were bystanders streamed by others. After participants finished writing, we invited them to verbally share their thoughts. During this process, we asked follow-up questions to probe the details, such as whether the streamer had notified the bystanders, how the bystanders realized the streaming, how streamers realized their bystanders were being streamed, the relationship between streamers and bystanders, and the actions streamers or bystanders took afterward. This activity allowed participants to reflect deeply on bystanders' privacy challenges, thus setting a foundation for the design ideation activity.

Design Ideation Activity Following the warm-up activity, each participant was asked to design informing features to address the privacy challenges they mentioned in the last step. Our focus on 'informing' was driven by its importance to bystanders shown in prior work [2, 35, 60] and aligned with our research questions. In the slide prompt for this step, we told them they were free to design the features in any way they desired, without the need to consider existing technical constraints. We chose the word 'feature' for its broad applicability, encompassing both technical and non-technical solutions. Participants were encouraged to propose any type of design, including software, hardware, policies, procedures, etc. For our in-person participants, each participant was given a large flip chart paper (25" x 30") as a mock-up interface for a computer, phone, or hardware that was commonly used in live streaming. They were also provided with a set of paper-based design widgets (e.g., webcam, speaker, screen sharing, virtual background, overlay, beauty filter, chatbot, buttons, toggles) and craft supplies (glue, scissors, marker, tape, and sticky notes). These items were intended to spark creativity and provide a starting point for the participants' designs. Participants could use any provided widgets or modify existing widgets. They were also asked to annotate each design decision. Our online participants utilized Figma, an interactive online whiteboarding tool, to create informing solutions. We provided a brief tutorial on using Figma to ensure our online participants were comfortable with the tool. Each participant was provided with an individual Figma account to design so that they would not be affected by other's design. All the widgets were made digitally available on Figma. After the design, each participant was asked to present their informing design and explain the design rationale. We also asked questions to probe details such as how the design addressed bystanders' privacy challenges, who initiated the design, and the limitations of using the feature. Participants in individual sessions completed the activities individually. Participants in group sessions first worked independently and then shared with others, facilitating collaborative brainstorming.

De-briefing At the end of the study, each participant was asked to revisit and modify their designs. If they made any modifications, they would be asked to clarify the rationale for each revision. Participants also reflected on how their informing designs could protect bystanders from privacy violations in live streaming.

3.3 Data Analysis

We employed thematic analysis [8] with an inductive approach to analyze the data. Our dataset consisted of the video recordings of the design ideation sessions (totaling 19 hours) and paper/digital prototypes that participants created. These video recordings were transcribed into text, and the prototypes were digitized for analysis. Four researchers with domain expertise in live streaming and privacy research engaged in the data analysis process. Each researcher first independently examined the transcribed texts and the elements in the prototype and identified initial codes. We then compared and discussed our initial codes and combined them into a single list, resulting in 96 codes. Based on the codes in the list, we placed all the codes on Miro (an online whiteboard) to examine the relationships and patterns between codes, collate similar codes, and identify themes after extensive discussions. In this process, we continuously revisited the dataset and refined the themes and sub-themes. The final thematic map consists of two primary themes: the considerations of bystanders and streamers in the informing process, and the design ideas desired by both bystanders and streamers for informing.

4 Results

Our results showed that both bystander and streamer participants were concerned that when being streamed by others, bystanders would suffer from: 1) personal details such as location or phone number being exposed to viewers, leading to unauthorized physical and virtual contact, 2) harmful actions from malicious audiences, including ridiculing, doxing, swatting, and stalking, 3) financial information like credit card details being accidentally revealed through streamer's webcam, and 4) the streaming of unfavorable moments, such as having a bad hair or poor game performance. Our findings align with prior research on bystanders' privacy concerns in live streaming [16,29,30]. Therefore, we did not delve deeply into these concerns but rather briefly introduced them here to set the stage for the upcoming sections. To protect bystanders from privacy violations, both streamer and bystander participants expressed their desire to be informed, and they also hoped the other party to be informed. Streamers wish to know if bystanders want to be included in the stream, and bystanders want to be informed if they are or will be part of the stream. However, our participants reported various challenges in informing, which have not been discussed in previous work and we will discuss them next.

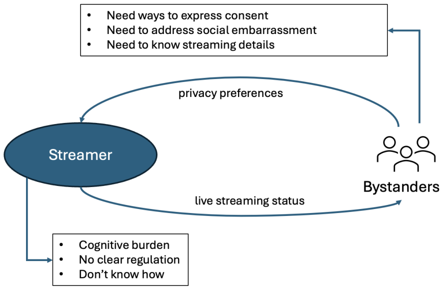


Figure 2: The bilateral communication informing loop

4.1 Needs, Challenges, and Constraints

Based on the interviews with streamers and bystanders, we found a bilateral communication loop in the informing process (Figure 2). Initially, streamers need to inform bystanders of the status of their live streaming. Once aware, bystanders then need to inform streamers of their privacy preferences, such as their willingness or concerns regarding being streamed. Bystanders (BS2[1], B5, B7, B11, B19, BS24, BS25) believed streamers should inform bystanders about the streaming status because bystanders often remain unaware of their inclusion in the stream, while streamers (BS6 and BS1) believed bystanders should inform streamers about their privacy preferences because streamers might not know bystanders' desire or reluctance to be streamed. However, there are challenges and constraints in this bilateral communication informing loop.

4.1.1 When Streamers Inform Bystanders of Their Live Streaming

Streamers have cognitive burdens. The real-time, multimodal, and socioeconomic nature of live streaming poses significant cognitive burdens on streamers to inform bystanders about the status of their live streaming. Our streamer participants (BS22, S23, BS25) agreed that as streamers, they needed to inform bystanders of their streaming activities. However, they were often deeply engaged in managing their performance, screensharing, audio/video input, and the synchronous interaction with their audience, to maintain a high quality of live streaming content. Given the real-time nature of their performance and interaction, streamers had to concentrate on the content they were broadcasting as they could not edit or withdraw the unwanted content. As such, streamers (S8, BS18, the streamers of BS4, BS6, BS24) sometimes forgot to notify bystanders in advance. As a result, our bystander participants (BS1, BS4, B11, B15, B19, BS24) shared that they were often informed after they had already been included in the stream, which made bystanders feel anxious. They often worried about whether they had said anything inappropriate

[1] "S" indicates the participant's self-reported role as a streamer, "B" indicates the participant's role as a bystander, and "BS" indicates that the participant is both a bystander and a streamer.

or done something 'stupid' (BS24) during the stream. Hence, streamers hoped they could be supported to inform the bystanders. For example, S8 said:

> I usually tell my parents I'm going to be busy, please don't come in during this time. But I think I forgot to let them know that day.

Informing bystanders is particularly burdensome in contexts involving large crowds such as public spaces. Streamers (S12, BS6) often found it burdensome and impractical to inform each bystander when they streamed in public settings because streamers were often preoccupied with their streaming activities and there were too many bystanders around to be informed. For example, S12 said:

> If in public, there're so many people around, I could see it being a burden if lots of people joining in and out and you tell them "hey, I'm streaming".

No clear regulations on informing. Our participants were uncertain about whether U.S. legislation permits or restricts live streaming in public spaces, and whether streamers are obligated to inform bystanders before their streams. The perceived lack of law clarity leads to varying opinions about whether informing should be given in public spaces. Some streamers (BS22, S23) and bystanders (BS2, B5, B16, BS25) believed that informing should occur regardless of lacking strict regulations for streaming in public spaces. These streamers acknowledged an ethical responsibility not to stream people randomly. These bystanders felt that streaming in public without informing them violated their portrait and privacy rights. However, some streamers (BS6) and even bystanders (BS1, BS24) felt streamers had the right to stream in public spaces and bystanders were not obligated to be notified because there were no regulation requirements. These different opinions indicate that clear regulations, policies and guidelines should be specified regarding informing bystanders. For example, BS1 (from bystander perspective) reported:

> I just had a quick question. I don't know if there's any legal framework behind streaming in public. Do you guys know anything? [...] But I feel like in public spaces, I think it's usually fine for you to just stream yourself. I don't think there's any legal restriction. I don't think there should be something that should be notified. I don't think I'm obligated to be notified.

Streamers struggle with how to inform bystanders. In most cases, streamers (S12, BS6, S23) did not know the bystanders. For instance, bystanders in public and online spaces are mostly strangers or passersby. Even when streamers wanted to inform their bystanders, they typically lacked the means to contact the bystanders, such as bystanders' phone numbers or social media accounts. For example, BS6 (from streamer perspective) reported:

> I'd tell them I'm streaming probably through a message if I had their number, but that hasn't always been the case.

Furthermore, our participants (BS1, BS2, B5, BS6, B7, B11, B19, BS24, BS25) reported that bystanders often lacked direct access to the streaming platform, making it impossible for streamers to reach each bystander within the streaming platform. For example, BS24 (from streamer perspective) said:

> Grant bystanders direct access to the streaming is challenging, since it would require them to log in as co-hosts, which goes against the intention of those who don't plan to be on the stream.

4.1.2 When Bystanders Inform Streamers of Their Privacy Preferences

After bystanders become aware of the potential to be exposed in a live stream, they need to inform streamers of their privacy preferences. During the process, they have to navigate through various challenges and require additional information to effectively communicate their preferences.

Bystanders need ways to clearly express their consent. Bystander participants (B5, B19, BS24, BS25) sometimes prefer to seek a more interactive consent process especially before they are captured in others' live streaming. They wanted to explicitly express their agreement or disagreement with being streamed to the streamers. With the consent, bystanders felt a sense of respect and might be more willing to be part of the streaming. Streamers could also realize bystanders' willingness or not and more effectively protect bystander privacy. However, bystanders often have limited ways to explicitly express their consent to streamers, unless the streamers intentionally ask for their consent. For example, B5 said:

> I've been streamed as focus, I was being asked pop-up quiz on campus, but that was with my consent. They approached me and asked me, 'would you want to be a part of this?' I said, 'sure, why not?', they asked me for my consent. This one I was asked and I said ok actually, so it was okay.

Bystanders need to cope with social embarrassment. Even when bystanders are approached to express their privacy preferences, they (BS2, B3, B5, B7, B11, BS25) frequently hesitated to explicitly communicate their privacy preferences with streamers due to social embarrassment. This hesitation was often rooted in politeness and a belief that they were not the primary focus, particularly when the streamers were unknown to them. When the streamer was known, bystanders also worried that such direct conversation might negatively influence the relationship between the known streamer and the bystander. Even when bystanders wanted to explicitly express their unwillingness, bystanders believed the streamers might misinterpret their concerns. As such, bystanders would choose implicit actions, such as dodging the camera and walking away, rather than directly talking to the streamer about their concerns. Some participants (BS1, BS6, B11) even favored merely informing without a clearly indicated consent to avoid direct interaction with streamers. Bystanders found a sense of "peace of mind" when they did not have to provide explicit consent. For example, B7 told us:

> What I'll do is to say, 'Hey, I really didn't like this'. Sometimes, they'll respond with, 'it's not that serious', 'don't take it so serious' or 'they didn't have any malicious intent'. They feel like I come after them and that's not what I'm trying to do.

However, streamer participants (BS6 and BS1) argued that without explicit communication, streamers might not know bystanders' reluctance to be streamed, nor take actions, such as adjusting the camera angle or relocating to a different area to avoid bystanders being streamed. Therefore, there needs an approach to deliver bystanders' privacy preferences to streamers without causing social embarrassment.

Bystanders need to know how they are streamed. Bystanders need details to make informed decisions on whether to be captured in others' live streaming. Streamers often did not provide detailed information about their streaming to bystanders, believing that bystanders were either not familiar with the concept of streaming or did not have access to the streaming platform that they use. However, bystanders (B3, BS4, B11, BS18, B19, BS25) expected more in-depth explanations, such as the specific streaming platforms being used, the devices being enabled, the intended audience, the live stream's topic, and the reasons for their inclusion as bystanders. Such detailed information was crucial for bystanders as it helped them to assess the potential reach of the stream and to understand how their presence might be interpreted or utilized in the stream, which are key to their privacy decisions. For instance, in private space, bystanders often have close proximity to the streamer's webcam and microphone, increasing the chance of their accidental appearance and voice capture in streams. So they wanted to know whether and how their appearance and voice could be captured. For example, BS18 (from bystander perspective) told us:

> I didn't know my roommate was streaming, and we shared a room. So I was just back from the gym and like the way his camera is set up, he can see like, the whole room is visible. So no matter when I come in or go out, he can see and everyone else can see it too. It'd be a good idea if he could just send a snapshot of how the webcam is placed and what it's capturing at the start of the stream.

This is also the case in online space. Streamers often stream on multiple streaming platforms to reach a wider audience and earn more money. As a result, bystanders are streamed on multiple platforms, thereby amplifying their exposure and privacy risks. Hence, bystanders need to know all the platform(s) where they are live streamed. For example, BS4 (from the bystander perspective) said:

> It'd be nice to know the streaming platform, cause if it's just streaming discord, I know it's just like three people watching, if on Twitch, it might be 300 people watching.

4.2 Desired Design Solutions

Given the needs, challenges and constraints reported in the above section, participants suggested various design solutions for the informing process to facilitate streamers to inform bystanders of their live streaming activities and also facilitate bystanders to inform streamers of their privacy preferences. In this section, we will introduce these design ideas.

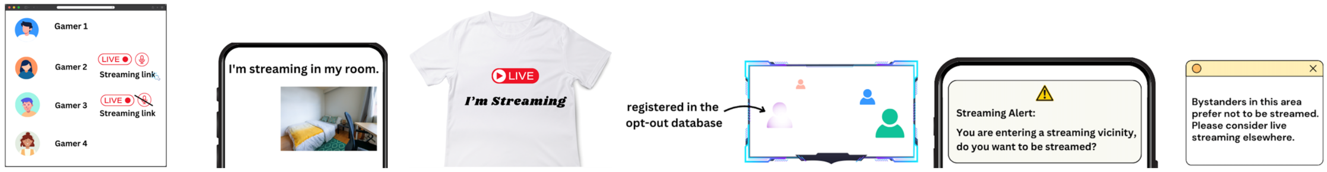
4.2.1 Platforms-Initiated Automatic Alerts

To reduce streamer's cognitive burden and minimize streamer's effort in informing bystanders, participants suggested that the live streaming platforms enable two types of automatic alerts for both streamers and bystanders:

Alerting streamers of bystanders' involvement. BS6 introduces an automated alert system for live streaming platforms designed to promptly inform streamers when a bystander is detected in their live streams within the physical environment. This system identifies bystanders via behavior or speech recognition techniques during the stream. Upon detection, streamers are alerted through a pop-up notification on their streaming device, highlighting the presence of a bystander. They can then take actions, such as informing the bystanders or avoiding bystanders being streamed. This feature requires no effort from bystanders and aims to make streamers aware of potential privacy violations to bystanders, particularly when streamers are busy with their live performances. With this automated alert, streamers can remain focused on their live performance, alleviating the need to constantly monitor for the involvement of bystanders. For example, BS6 explained based on his streamer experience:

> If I was actively playing a game, then it's hard to realize there is a bystander in that case. If I had to send them notifications all individually, I think that would probably get too complex to manage. One option could be to have the streaming platform do that detection for you. And if it notices certain behavior or certain words being said, it could pop up a notification saying like 'someone getting in'.

Alerting bystanders before streaming. Our participants introduced an automatic alert feature designed to notify bystanders within the virtual environment when streamers start live streaming. This system requires bystanders to proactively


Gamer 1
Gamer 2
LIVE
Streaming link
Gamer 3
LIVE
Streaming link
Gamer 4
I'm streaming in my room.
LIVE
I'm Streaming
registered in the opt-out database
Streaming Alert:
You are entering a streaming vicinity, do you want to be streamed?
Bystanders in this area prefer not to be streamed. Please consider live streaming elsewhere.

a) Provide gamers a link to the streamers' streaming channel

b) Send bystanders a pre-recorded message along with a snapshot of the streaming area

c) Ask the streamer to wear t-shirts about the streaming

d) Bystanders register in a opt-out database to be auto-blurred when they enter the streaming

e) Bystanders receive an automated SMS notification, and their consent responses are aggregated into a notification for the streamer.

Figure 3: Examples of participants' design. We used Canva (an online protyping platform: https://www.canva.com/) to digitally translate the paper-based sketches created by the participants.

follow streamers, such as their roommates, gaming partners, and friends, who might inadvertently capture and broadcast their personal information during live streams. Once these followed streamers initiate a live stream, the bystanders immediately receive a notification from the platform, ensuring they are aware of the streaming activity without relying on the streamers to inform them manually, who might be preoccupied with their performance. Streamers are only required to guide their potential bystanders on how to follow their streaming accounts. With this setup, every time streamers go live, the platform automatically alerts the bystanders, allowing streamers to focus on their content without the need to individually notify each bystander. For example, B10 suggested:

> You can follow people on Twitch. This feature is useful if your friends in the game are also your friends on Twitch. For instance, if I follow my buddy on Twitch and he starts streaming, I would get a notification on my phone through Twitch, alerting me, 'Hey, your buddy is streaming.' This happens even if he doesn't directly tell me.

4.2.2 Platform-Enforced Regulation and Policy

To mitigate the uncertainty surrounding legal and policy requirements about streamers' obligations to notify bystanders who are within the physical environment before streaming them, participants recommended the establishment of explicit policies. These policies could be enforced through legislation or platform guidelines, such as terms of conduct, community guidelines, or tutorials for new streamers. The policies should clarify whether streamers are required to inform bystanders and obtain explicit consent from bystanders, especially in public spaces. This approach aims to legally protect bystanders' privacy and ensure ethical streaming practices by clearly defining the informing responsibilities of streamers towards bystanders. For example, BS2 (from bystander perspective) said:

> Maybe like a policy the streamer has to agree to. You have to get consent before you stream anybody or something.

4.2.3 Embedded Communication Channels to Inform

As streamers reported challenges in delivering their informing to the bystanders, and bystanders also struggled with ways to express their consent, participants designed a series of communication channels embedded or linked with the live streaming platforms to assist with the informing:

One-to-one messaging between streamers and bystanders. Participants suggested implementing a two-way one-on-one messaging feature within live streaming platforms. This feature would facilitate communication between streamers and bystanders who are within the physical environment in two main scenarios: informing bystanders about live streaming activities and allowing bystanders to convey their privacy preferences to streamers. When streamers plan to go live and wish to notify bystanders, they can request the platform to send a notification message directly to those bystanders. If the bystanders are registered users of the platform, BS17 proposed that bystanders could receive this notification through an in-platform message, enabling streamers to inform them without needing to access their private contact information. Bystanders can then respond within the same platform, stating their privacy preferences clearly and directly:

> I share kitchen space with my roommate. I came into the kitchen to make myself some stuff to eat. I had no idea she was streaming (B15's concern)

> Her roommate can tag her [...] Similar to Facebook tagging or identity of that person and then send the person a notification. (BS17's design)

For bystanders not registered with the platform, i.e., they have not installed the app or are unfamiliar with live streaming, B5 proposed a GPS-based SMS feature (Figure 3(e)) to provide a communication channel between streamers and bystanders. Streamers would first input their streaming location. Bystanders who are nearby would then receive an automated SMS notification stating, "You are entering a streaming vicinity, do you want to be streamed?". This approach necessitates collaboration between platforms and government or service providers to send automated SMS alerts to bystanders. Such collaboration could effectively communicate the consent process to a broad audience swiftly and directly, bypassing the need for streamers and bystanders to exchange contact information. The system also allows bystanders to respond with their consent. These responses could be aggregated into an average approval rating for the area, which will serve as a guide for streamers to gauge general bystander consent:

> I thought of a feature, which is like a GPS-based authentication thing for crowd streaming [...] We all receive some SMS alerts when the hurricane or kidnapping happens, because we are in this sort of area which was impacted by it. We could approach the government and don't have to ask anybody for their number, you just send them an alert, they can choose whether they approve of been seen or not [...] Definitely it's not possible to go and ask everybody for the approval, but we'll take an average. If the on average approval rating is quite low, then the streamer must probably reconsider doing it somewhere else.

Both one-on-one messaging functions eliminate the need for streamers and bystanders to collect each other's personal contact information, streamlining the process of informing. It also offers bystanders a straightforward method to articulate their privacy preferences, ensuring they have a say in whether they want to be included in live streams. Additionally, the one-on-one messaging feature guarantees that notifications are delivered and seen, even if streamers or bystanders are otherwise occupied, thereby enhancing the effectiveness of communication between streamers and bystanders.

One-way one-to-many indicator. Aside from the messaging communication channels, participants also suggested one-way one-to-many channels to inform bystanders through visual or auditory indicators. Such indicators can be physical or virtual indicators initiated by streamers. Once activated, it will notify broad bystanders about the streaming status through visual or auditory cues. The indicator is independent of sending individual notifications to bystanders, as in public settings and online gaming scenarios, it is ineffective to individually message a substantial number of passersby and online players who keep coming and going in others' live streams.

The physical indicators include visual cues, such as flashing lights (S17, BS18) and conspicuous signs (B5), alongside auditory signals, such as a beep sound (S17). The indicators could be incorporated as a software feature enforced by the streaming platform or activated manually through a button on streaming devices by streamers when the streaming starts. They might even be integrated as a sign on the T-shirt (Figure 3(c)). The virtual indicators can be a "live" icon displayed around the game avatar of the streamers who are streaming. The icons are mandatory before streamers start their streaming online. These indicators help streamers inform the bystanders of live broadcasts without the need to obtain bystanders' contact information. For example, B5 reported:

> I think that's a good start to make streaming obvious because if it's a busy place, you can't really go and notify everybody and people keep coming and going. Maybe ask the streamer to wear t-shirts about the streaming.

However, our participants also acknowledged that the effectiveness of physical indicators could be influenced by the surrounding environment. Visual cues, for example, can become less effective in well-lit daytime environments where they might blend into the background, making it difficult for bystanders to notice them. Furthermore, there are concerns raised by some participants regarding auditory signals, which they find to be annoying. For example, B2 said:

> Because like you said, the blinking lights, right? But if it's daytime, right? Sunny, how are you going to see the lights? So stuff like that. That's why I said like, it's kind of difficult to implement it. And that's what I mean.

This highlights the necessity of designing indicators that are less intrusive and consistently recognizable, regardless of the environmental conditions they are subjected to.

4.2.4 Embarrassment-Free Bystander Privacy Expression

To mitigate the social discomfort bystanders may experience when expressing their privacy preferences not to be included in others' live streams, two embarrassment-free mechanisms for bystanders' privacy preference expression were proposed.

Bystanders' one-sided opt-out. To accommodate those who wish to remain outside the scope of live streams, an opt-out mechanism (Figure 3(d)) has been proposed by our participants. This mechanism is designed for bystanders who are within the physical environment. Bystanders can register in a database provided by the platform or a third party, entering specific personal details that can recognize their identities. Upon registration, the system is designed to recognize these bystanders whenever they appear in others' live streams, automatically applying blurring or muting effects to their likeness or voice. This approach eliminates the need for any direct communication between bystanders and streamers, thereby sparing bystanders from the potential awkwardness of confronting streamers about their privacy preferences. For example, BS6 (from streamer perspective) reported:

> There's also the idea of on a platform-wide level, maintaining an opt-out type database of people who don't want to be seen on any stream ever. So what you could do is have any stream search through that database, but constantly cross-reference between the people it sees in the stream. If someone shows up that's in the database, automatically blur them out and mute them.

Device-enforced consent-based protection. To further alleviate the discomfort of bystanders in expressing their privacy preferences directly to the streamers, a device-enforced consent-based mechanism is proposed for bystanders who are within the physical environment. This feature automates the blurring of bystanders in live streams based on their consent, operating at the device level. When a streaming device, such as a camera or a microphone, detects a bystander, it triggers a notification to the bystander requesting their consent to be included in the stream. Should the bystander agree, they will appear unaltered; if they decline, the device will automatically blur their presence in the live stream. This method addresses bystanders' concerns that voicing their reluctance to participate might be perceived as impolite, lead to social embarrassment, or be disregarded by the streamers. By sending the consent to the device, rather than to the streamer, bystanders can assert their preferences without fear of personal conflict or judgment. The device-level enforcement ensures that bystanders' privacy preferences are respected as they are, granting them greater control and reducing the likelihood of misunderstanding. For example, B19 expressed:

> Streamer starts the live stream, and then people around the person where the camera can see clearly get an alert, like you have entered a live streaming vicinity. And then the bystanders can be asked if they are willing to join, because there are sometimes bystanders want to join. There are some people, sometimes people like being on camera, like being a part of something, if they like the streaming topic. And depending on that, they will be blurred out or no. If they want to be in the live stream, then they don't need to be blurred out.

4.2.5 Providing Details in Streamer's Informing

Bystanders require comprehensive details about the live streams in which they are to be captured to make informed decisions regarding their privacy preferences. They have voiced a need for detailed information on how, where, and why they are streamed. Irrespective of the method used by streamers to inform them — be it through a message, indicator, or alert — bystanders wish to be informed about the particular streaming platforms in use, the devices utilized for streaming, the target audience, the subject matter of the live stream, and the rationale behind their inclusion as bystanders. This information is crucial for them to make informed consent decisions. For example, in the case of a virtual indicator, bystanders expect it to provide a link to the streaming channel (Figure 3(a)). This link should clearly indicate whether the streaming is occurring on the same platform, a different one, or across multiple platforms. The link serves not only to give online bystanders an easy way to see how they appear in the stream but also to understand the potential audience size. For instance, BS4 (from bystander perspective) proposed:

> [...] Right now, like discord, only sees if you're streaming on discord. You could join discord and not know if your friend is streaming on Twitch. The design I have was like a streamer mode for streamers. They have to enable the streamer mode to go live [...] For example, User1 is my friend. He's streaming on Twitch. I load up discord. It would show me he's in the voice chat. He's streaming on a different platform. Streamer could also give you the link of their channel. If you click on it, you could see the streaming status. I think that would be a good idea. I'm sure streamers would like that too, because then people can click and they need more audience.

If the notification comes as a message, our bystander participants within the physical environment recommend it include a pre-recorded message saying, "I'm streaming," along with a snapshot of the streaming area (Figure 3(b)). This feature allows bystanders to actively avoid areas where they might be captured on camera if they prefer not to be included in the live stream. It empowers them to navigate their environment with greater confidence and without the constant fear of unintentionally appearing in a live stream. For example, BS18 (from bystander perspective) said:

> I didn't know my roommate was streaming, and I just went into the room. So there might be a pre-recorded message like 'I'm streaming in my room' sent by a toggle bar. When they start streaming, they just send a snapshot of how the webcam is placed and what it's capturing. You can just avoid that area in particular, and just do everything that you want to do, and it's not being that area.

5 Discussion

Our study explores the reciprocal informing practices between streamers and bystanders in live streaming from both perspectives. Based on participants' design ideas, we propose three key design principles to enhance bilateral informing interaction in synchronous information disclosure.

Contextualizing informing process. Contextualizing is not a novel concept. Previous research has shown that privacy notices and choices should be tailored to contextual factors such as space, timing, channel, and modality [17,56]. This has been supported by prior work in synchronous information disclosure like IoT and AR, which considers contextual factors like environments (e.g., home, Airbnb) and pre-existing relationships between the owner and bystanders (e.g., host and guest) [2,37,52,60]. Our findings in live streaming also highlight the importance of environments and relationships for informing. For example, when device owners and bystanders are unknown to each other, participants prefer one-to-many indicators in public spaces. In private spaces, with known contacts, one-on-one messages are preferred. In online spaces, where bystanders might be streamed on different streaming platforms, notices could be sent across various platforms.

Our contribution extends beyond prior work by emphasizing the **social and interpersonal nature** when contextualizing the informing process. The informing processes should adapt to the social contexts, considering factors such as the target audience, group size, and activities or status of stakeholders. For example, streamers might interact with a small, known group of viewers or a large, anonymous public audience. In cases of large and unknown audiences, it is crucial for bystanders to be informed about their visibility and data sharing. Additionally, the current activity and status of stakeholders, especially device owners, should be considered. Our findings indicate that streamers have to manage multiple activities, including performing, interacting with numbers of unknown audiences, and addressing context changes, which leads to a significant cognitive burden that may hinder their ability to notice and protect bystanders effectively. Thus, automated notifications that consider social aspects are necessary.

These contextual factors could also implicate other synchronous information disclosure contexts beyond live streaming. For example, bystanders might be involved when IoT users share recordings from their smart cameras with their friends, family members, and online social networks, thus expanding bystanders' exposure to different types of audiences. AR users might be preoccupied with interacting with other users and may not easily realize bystanders' unwillingness when bystanders pass by the device. Therefore, our design principles could contribute to other synchronous scenarios. We recommend that designers consider both the informing mechanisms for different contexts and the social and interpersonal nature of the informing process.

Balancing the power dynamic between streamer and bystander through mutual transparency. Our results highlight that the power dynamic between streamers and bystanders is unbalanced. Although there are bilateral informing needs, streamers need to initiate the informing process as bystanders often lack agency over their privacy. Bystanders rely on streamers for information and decision-making. Without streamer initiation, bystanders often lack awareness of being streamed and cannot make informed decisions. They expressed a desire for greater transparency, such as knowing the number of audience members, their presentation in the streams, and the streamers' attitudes toward their participation. Moreover, without explicit communication from bystanders about their privacy preferences, streamers remain unaware of bystanders' desires to participate or their level of comfort, exacerbating the power imbalance. Therefore, mutual transparency in the informing process is crucial, enabling both parties to make informed decisions and protect bystander privacy effectively.

To empower bystanders, previous informing designs in synchronous information disclosure, such as IoT, have enhanced transparency by detailing which devices are collecting data, what data is being collected, and whether data collection is active [2, 37]. Our research aligns with these findings. For instance, our bystanders also wanted to know if streaming is active and whether the streamer is using a camera or engaging in voice chat.

Our unique contribution emphasizes **mutual transparency** to reduce the power imbalance between bystanders and streamers by ensuring both parties have agency and are informed about crucial details, such as platform or legal policies, data recipients, social implications, and participation details. For instance, informing both bystanders and streamers about the platform or legal policies is especially important on online platforms and in public spaces where clear informing practices are often lacking. Without clear regulations, both parties may be unaware of bystanders' rights and streamers' obligations. It is also important to inform bystanders about data recipients, as live streaming involves broad, nontransparent, anonymous, and public audiences. Bystanders need to know who is receiving their data and on which platform. Additionally, providing information about social implications allows bystanders to manage their self-presentation to the audiences; for example, one bystander wanted to know how the streamer's audience commented on him. Lastly, informing streamers about bystanders' detailed participation information helps streamers understand if bystanders are willing to be part of the streaming, how much they want to participate, and in what streaming topics they want to be involved. These transparency details can also benefit other synchronous information disclosure contexts. For example, in the case of wearable health devices used in fitness centers, it is crucial to inform device owners and bystanders about who has access to the collected health data, the legal policies governing its use, the social implications of wearing such devices in public, and whether bystanders are comfortable being recorded or included in data collection.

While enhancing these details of the informing process, it is vital to consider that some bystanders may lack access to or interest in the streaming platform, limiting their control over their privacy. Therefore, informing practices should be transparent and effective without burdening bystanders, such as through visible indicators (i.e., one-way one-to-many indicators) or familiar communication methods (i.e., text messages) that do not require downloading an extra streaming platform. This consideration also contributes to other synchronous information disclosure contexts. For example, when a bystander is involved in AR interactions by AR users, bystanders might not be able to gain access to the AR device. In this case, informing practices should utilize methods that are easily accessible and do not impose additional steps on bystanders, ensuring their awareness and consent without requiring direct interaction with the AR device.

Mediating communication barriers between streamer

and bystander. Our findings reveal that the informing design should mediate the communication barriers between streamers and bystanders, especially through third parties such as platforms or government agencies. Our streamers want bystanders to inform them of bystanders' privacy preferences, but bystanders often feel embarrassed to confront streamers directly or do not trust the streamers' decisions in protecting bystander privacy. Our bystanders expect streamers to respect their privacy, but streamers might not do so because they assume bystanders are fine with being streamed or make decisions on behalf of bystanders at that point. Thus, **third-party mediation**, such as device or platform-enforced informing designs, can play important roles in mediating the communication barriers between streamers and bystanders.

Prior informing designs in synchronous information disclosure such as IoT have enabled bystanders to communicate with device owners about their privacy preferences or to circumvent device owners to make their own privacy decisions through mechanisms such as bystander mode [60] or guest accounts [37]. But do bystanders prefer to use these controls? Our findings in live streaming highlighted that bystanders sometimes do not prefer direct communication or control because bystanders felt it was bothersome to take extra steps to communicate with streamers, especially when they do not have easy access to the device. They also worried that such actions might be interpreted as impolite by unknown streamers or negatively influence their relationship with known streamers. However, they also do not want streamers' personal decisions or adjustments to override or influence their willingness to participate or be involved. Therefore, our participants proposed device/platform-enforced informing mechanisms such as opt-out database, platform-initiate alerts, platform-enforced policy, and device-enforced consent-based protection to provide assurance and fairness for bystander privacy without relying on streamers' subjective decisions.

Prior informing work in live streaming [16] also proposed using an opt-out database, but researchers proposed it from a one-sided perspective by providing bystanders with low-effort notifications. In contrast, our participants developed the opt-out database to address the communication barriers between the two stakeholders from a two-way perspective. Specifically, it is designed by our streamers to tackle bystanders' social embarrassment when expressing unwillingness to be streamed. It involves streamers actively recognizing and respecting bystanders' privacy preferences while also allowing bystanders to communicate preferences without direct confrontation. This approach demonstrates mutual privacy consideration, showing that one stakeholder group sincerely values the privacy and social needs of the other, emphasizing that bystander privacy protection requires collaboration among stakeholders. It highlights promising opportunities for cooperation and coordination between stakeholders in live streaming. Such two-way third-party mediators also have implications for other synchronous information disclosure contexts. For example, bystanders might not feel comfortable directly communicating with AR users about their privacy concerns; thus, they could register their preferences not to be recorded, and the AR system would automatically blur their image or mute their voice, respecting their privacy without direct confrontation.

6 Limitation

First, our study concentrated on the ideation phase to foster innovative design ideas to address informing challenges regarding bystander privacy in live streaming. However, it did not include subsequent stages, such as prototype development and evaluation, which could have provided practical and validated design solutions. Future studies may implement and test the proposed ideas if technological advances allow.

Second, although we aimed to include at least two participants per sessions, representing both streamers and bystanders, but unforeseen absences led to some sessions with a single participant. While designing with one participant is common in prior work [32, 33], and can provide detailed individual insights [62]. But the varying group sizes may have affected the ideation outcomes and limited the diversity of of perspectives. Future work could aim to standardize group sizes to ensure more consistent and comprehensive insights.

Third, despite efforts to recruit participants through various platforms, most of our participants were college students. This might be because our study was conducted at the university. People with different professions or educational backgrounds may have different perceptions and practices related to managing bystanders' privacy. Therefore, our sample may not fully capture the perspectives of streamers and bystanders with different occupations or educational backgrounds.

Fourth, although we targeted participants from various disciplines, we had more CS students (43%) than non-CS (33%), with 5 participants not disclosing their majors. Since CS students tend to be more tech-savvy, our results might not accurately reflect the privacy needs of non-CS users. Future research could include participants from more diverse backgrounds to broaden the applicability of our findings.

7 Conclusion

In this paper, we engaged 21 streamers and bystanders to understand their mutual expectations for the informing process regarding bystander privacy in live streaming. The results suggested that both streamers and bystanders face a variety of challenges during the informing process in live streaming. Based on these insights, our participants proposed various design ideas for informing streamers and bystanders to protect bystander privacy. From these concepts, we summarized key design principles that can guide the development of future technologies in this area.

References

[1] Imtiaz Ahmad, Taslima Akter, Zachary Buher, Rosta Farzan, Apu Kapadia, and Adam J Lee. Tangible privacy for smart voice assistants: Bystanders' perceptions of physical device controls. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–31, 2022.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–28, 2020.

[3] Gulsum Akkuzu, Benjamin Aziz, and Mo Adda. Towards consensus-based group decision making for co-owned data sharing in online social networks. *IEEE Access*, 8:91311–91325, 2020.

[4] Rawan Alharbi, Mariam Tolba, Lucia C Petito, Josiah Hester, and Nabil Alshurafa. To mask or not to mask? balancing privacy with visual confirmation utility in activity-oriented wearable cameras. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 3(3):1–29, 2019.

[5] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. {Bystanders'} privacy: The perspectives of nannies on smart home surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[6] Andrew Besmer and Heather Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1563–1572, 2010.

[7] Bitdefender. What are Private Data Leaks. https://www.bitdefender.com/cyberpedia/what-are-private-data-leaks, 2022.

[8] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[9] Chia-Chen Chen and Yi-Chen Lin. What drives live-stream usage intention? the perspectives of flow, entertainment, social interaction, and endorsement. *Telematics and Informatics*, 35(1):293–303, 2018.

[10] Hichang Cho and Anna Filippova. Networked privacy management in facebook: A mixed-methods and multinational study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 503–514, 2016.

[11] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M Jose. Bystander privacy in lifelogging. In *Proceedings of the 30th International BCS Human Computer Interaction Conference 30*, pages 1–3, 2016.

[12] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "i would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 2021.

[13] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y Charlie Hu, and Bo Ji. Bystandar: Protecting bystander visual data in augmented reality systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, pages 370–382, 2023.

[14] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2377–2386, 2014.

[15] Mariella Dimiccoli, Juan Marín, and Edison Thomaz. Mitigating bystander privacy concerns in egocentric activity recognition with deep learning and intentional image degradation. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(4):1–18, 2018.

[16] Cori Faklaris, Francesco Cafaro, Asa Blevins, Matthew A O'Haver, and Neha Singhal. A snapshot of bystander attitudes about mobile live-streaming video in public settings. In *Informatics*, volume 7, page 10. MDPI, 2020.

[17] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[18] Ricard L Fogues, Pradeep K Murukannaiah, Jose M Such, and Munindar P Singh. Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 24(1):1–29, 2017.

[19] Johann N Giertz, Welf H Weiger, Maria Törhönen, and Juho Hamari. Content versus community focus in live streaming services: How to drive engagement in synchronous social media. *Journal of Service Management*, 33(1):33–58, 2022.

[20] Rakibul Hasan. Reducing privacy risks in the context of sharing photos online. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2020.

[21] Rakibul Hasan, David Crandall, Mario Fritz, and Apu Kapadia. Automatically detecting bystanders in photos to reduce privacy risks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 318–335. IEEE, 2020.

[22] Noe Vargas Hernandez, Jami J Shah, and Steven M Smith. Understanding design ideation mechanisms through multilevel aligned empirical studies. *Design studies*, 31(4):382–410, 2010.

[23] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 103–112, 2011.

[24] Haiyan Jia and Heng Xu. Autonomous and interdependent: Collaborative privacy management on social networking sites. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4286–4297, 2016.

[25] Ben Jonson. Design ideation: the conceptual sketch in the digital age. *Design studies*, 26(6):613–624, 2005.

[26] Marion Koelle, Katrin Wolf, and Susanne Boll. Beyond led status lights-design requirements of privacy notices for body-worn cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*, pages 177–187, 2018.

[27] Jacob Kramer-Duffield. *Beliefs and uses of tagging among undergraduates*. The University of North Carolina at Chapel Hill, 2010.

[28] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3217–3226, 2011.

[29] Yao Li, Yubo Kou, Je Seok Lee, and Alfred Kobsa. Tell me before you stream me: Managing information disclosure in video game live streaming. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–18, 2018.

[30] Zhicong Lu, Michelle Annett, and Daniel Wigdor. Vicariously experiencing it all without going outside: A study of outdoor livestreaming in china. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–28, 2019.

[31] Zhicong Lu, Haijun Xia, Seongkook Heo, and Daniel Wigdor. You watch, you give, and you engage: a study of live streaming practices in china. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–13, 2018.

[32] Yuhan Luo, Peiyi Liu, and Eun Kyoung Choe. Co-designing food trackers with dietitians: Identifying design opportunities for food tracker customization. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[33] Stephann Makri, Tsui-Ling Hsueh, and Sara Jones. Ideation as an intellectual information acquisition and use context: Investigating game designers' information-based ideation behavior. *Journal of the Association for Information Science and Technology*, 70(8):775–787, 2019.

[34] Ameera Mansour and Helena Francke. Collective privacy management practices: A study of privacy strategies and risks in a private facebook group. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–27, 2021.

[35] Shady Mansour, Pascal Knierim, Joseph O'Hagan, Florian Alt, and Florian Mathis. Bans: Evaluation of bystander awareness notification systems for productivity in vr. In *Network and Distributed Systems Security (NDSS) Symposium*, 2023.

[36] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proc. Priv. Enhancing Technol.*, 2020(2):436–458, 2020.

[37] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. "you offer privacy like you offer tea": Investigating mechanisms for improving guest privacy in iot-equipped households. 2022.

[38] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. " i don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, pages 1–11, 2020.

[39] Mark McGill, Daniel Boland, Roderick Murray-Smith, and Stephen Brewster. A dose of reality: Overcoming usability challenges in vr head-mounted displays. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2143–2152, 2015.

[40] Francesca Mosca and Jose M Such. Elvira: An explainable agent for value and utility-driven multiuser privacy. In *Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems*, pages 916–924, 2021.

[41] Josh Nadeau. Banking and Finance Data Breaches: Costs, Risks and More To Know. https://securityintelligence.com/articles/banking-finance-data-breach-costs-risks/, 2021.

[42] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. "i thought you were okay": Participatory design with young adults to fight multiparty privacy conflicts in online social networks. In *Designing Interactive Systems Conference (DIS)*, 2021.

[43] Jan Nolin and Nasrine Olson. The internet of things and convenience. *Internet Research*, 26(2):360–376, 2016.

[44] Farzad Nourmohammadzadeh Motlagh, Seyed Ali Alhosseini, Feng Cheng, and Christoph Meinel. An approach to multi-party privacy conflict resolution for co-owned images on content sharing platforms. In *Proceedings of the 2023 8th International Conference on Machine Learning Technologies*, pages 264–268, 2023.

[45] Joseph O'Hagan, Mohamed Khamis, Mark McGill, and Julie R Williamson. Exploring attitudes towards increasing user awareness of reality from within virtual reality. In *ACM International Conference on Interactive Media Experiences*, pages 151–160, 2022.

[46] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4):1–35, 2023.

[47] Joseph O'Hagan and Julie R Williamson. Reality aware vr headsets. In *Proceedings of the 9th ACM international symposium on pervasive displays*, pages 9–17, 2020.

[48] Seonghun Park, Jisoo Ha, Jimin Park, Kyeonggu Lee, and Chang-Hwan Im. Brain-controlled, ar-based home automation system using ssvep-based brain-computer interface and eog-based eye tracker: A feasibility study for the elderly end user. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 31:544–553, 2022.

[49] Sunyup Park, Anna Lenhart, Michael Zimmer, and Jessica Vitak. " nobody's happy": Design insights from {Privacy-Conscious} smart home power users on enhancing data transparency, visibility, and control. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023.

[50] Alfredo J Perez, Sherali Zeadally, Scott Griffith, Luis Y Matos Garcia, and Jaouad A Mouloud. A user study of a wearable system to enhance bystanders' facial privacy. *IoT*, 1(2):13, 2020.

[51] Sandra Petronio. Brief status report on communication privacy management theory. *Journal of Family Communication*, 13(1):6–14, 2013.

[52] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, et al. Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras. In *Designing Interactive Systems Conference*, pages 26–40, 2022.

[53] Blaine A Price, Avelie Stuart, Gul Calikli, Ciaran Mccormick, Vikram Mehta, Luke Hutton, Arosha K Bandara, Mark Levine, and Bashar Nuseibeh. Logging you, logging me: A replicable study of privacy and sharing behaviour in groups of visual lifeloggers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(2):1–18, 2017.

[54] Leslie Ramos Salazar. Be Careful What you Post: Social Media and Reputation, 2021. https://profspeak.com/be-careful-what-you-post-social-media/, 2021.

[55] Kavous Salehzadeh Niksirat, Diana Korka, Hamza Harkous, Kévin Huguenin, and Mauro Cherubini. On the potential of mediation chatbots for mitigating multiparty privacy conflicts-a wizard-of-oz study. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–33, 2023.

[56] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*, pages 1–17, 2015.

[57] Katrin Scheibe, Franziska Zimmer, Kaja Fietkiewicz, and Wolfgang Stock. Interpersonal relations and social actions on live streaming services. a systematic review on cyber-social relations. 2022.

[58] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. You are being watched: Bystanders' perspective on the use of camera devices in public spaces. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 3197–3203, 2016.

[59] John C Tang, Gina Venolia, and Kori M Inkpen. Meerkat and periscope: I stream, you stream, apps stream for live

streams. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 4770–4780, 2016.

[60] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. “it would probably turn into a social faux-pas”: Users’ and bystanders’ preferences of privacy awareness mechanisms in smart homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2022.

[61] F Ted Tschang and Janusz Szczypula. Idea creation, constructivism and evolution as key characteristics in the videogame artifact design process. *European management journal*, 24(4):270–287, 2006.

[62] Froukje Sleeswijk Visser, Pieter Jan Stappers, Remko Van der Lugt, and Elizabeth BN Sanders. Contextmapping: experiences from practice. *CoDesign*, 1(2):119–149, 2005.

[63] Pamela Wisniewski, Heather Lipford, and David Wilson. Fighting for my space: Coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 609–618, 2012.

[64] Yanlai Wu, Xinning Gui, Pamela J Wisniewski, and Yao Li. Do streamers care about bystanders’ privacy? an examination of live streamers’ considerations and strategies for bystanders’ privacy management. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–29, 2023.

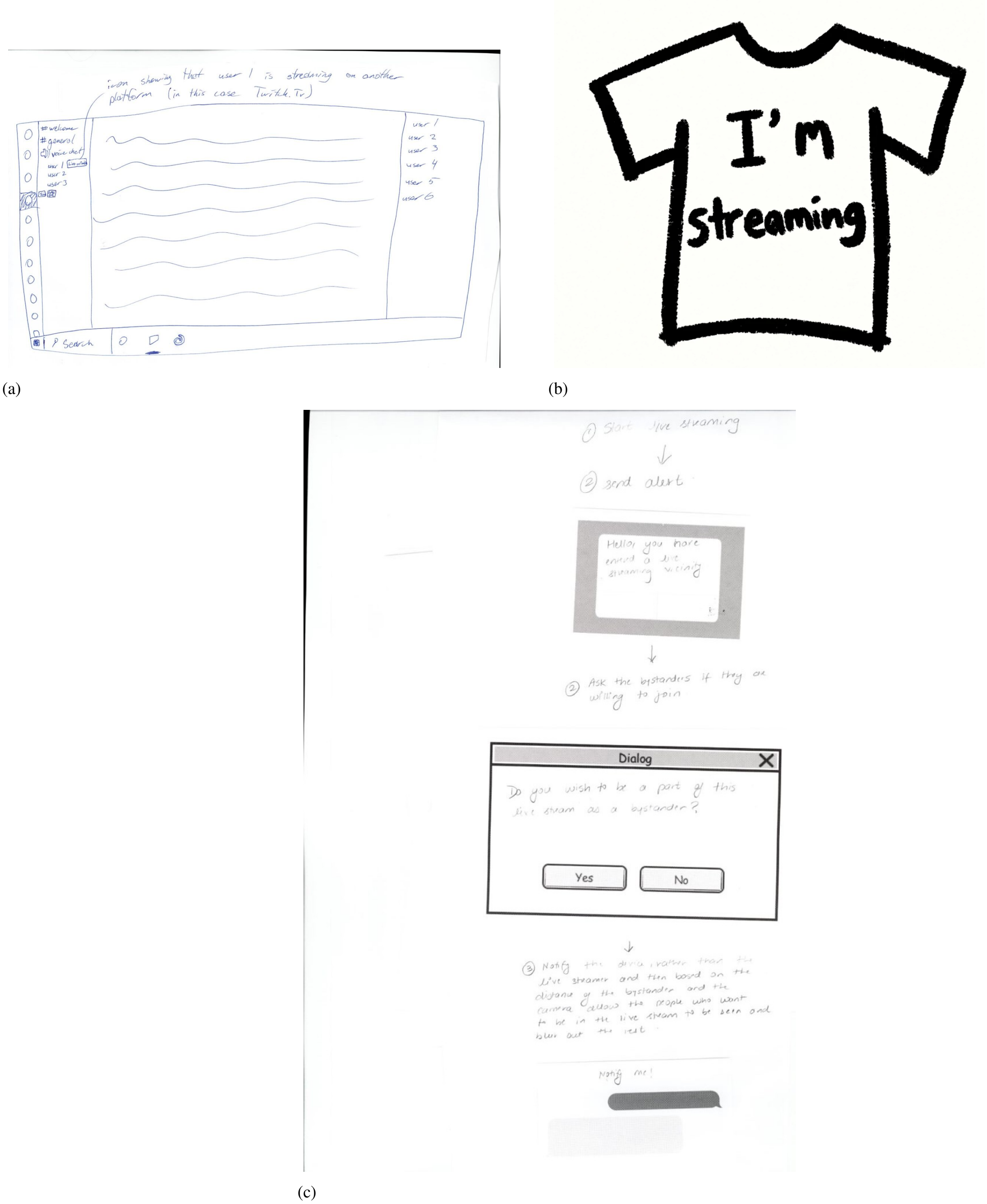
[65] Yanlai Wu, Yao Li, and Xinning Gui. " i am concerned, but...": Streamers’ privacy concerns and strategies in live streaming information disclosure. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–31, 2022.

[66] Kaihe Xu, Yuanxiong Guo, Linke Guo, Yuguang Fang, and Xiaolin Li. My privacy my decision: Control of photo sharing on online social networks. *IEEE Transactions on Dependable and Secure Computing*, 14(2):199–210, 2015.

[67] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Free to Fly in Public Spaces: Drone Controllers’ Privacy Perceptions and Practices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI ’17, pages 6789–6793, New York, NY, USA, 2017. Association for Computing Machinery.

[68] Tengfei Zheng, Tongqing Zhou, Qiang Liu, Kui Wu, and Zhiping Cai. Characterizing and detecting non-consensual photo sharing on social networks. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 3209–3222, 2022.

Appendix A Examples of Participants' Original Designs.



(a)

icon showing that user 1 is streaming on another platform (in this case Twitch.Tv)

(b)

(c)

① Start live streaming

② send alert

Hello, you have entered a live streaming vicinity

② Ask the bystanders if they are willing to join

Do you wish to be a part of this live stream as a bystander?

③ Notify the device, rather than the live streamer and then based on the distance of the bystander and the camera allow the people who want to be in the live stream to be seen and blur out the rest.

Notify me!

Figure 4: (a)provide gamers a link to the streamers' streaming channel (b)ask the streamer to wear t-shirts about the streaming (c)bystanders receive an automated SMS notification, and their consent responses are aggregated into a notification for the streamer.

Appendix B Demographics of Participants.

Session	#	Gender	Occupation	Major	Bystander /Streamer	Streaming Topics	Stream Who	Where being Streamed	Streamed by Who
1(in person)	1	Male	Student	N/A	Bystander &Streamer	Valorent	Online Bystanders	In Game	Online Friend
	2	Male	Student	N/A	Bystander &Streamer	Outdoor Activities	Public Bystanders	At Bar	Unknown Streamer
2 (in person)	3	Male	Student	CS	Bystander	N/A	N/A	On Campus	Friend
	4	Male	Student	N/A	Bystander &Streamer	Overwatch	Online Bystanders	In Game	Online Friend & Opponent
3 (in person)	5	Female	Student	CS	Bystander	N/A	N/A	On Campus& In Farmers Market	Unknown Streamer
	6	Male	Student	CS	Bystander &Streamer	NBA 2K	Roommate	In Public	Unknown Streamer
4 (online)	7	Male	Student	CS	Bystander	N/A	N/A	In Game	Online Friend
	8	Male	Student	EC	Streamer	Casual Game	Parent	N/A	N/A
5 (in person)	10	Male	Student	EE	Bystander	N/A	N/A	In Game	Online Friend
6 (in person)	11	Male	Student	N/A	Bystander	N/A	N/A	On Campus	Unknown Streamer
7 (in person)	12	Male	Student	CS	Streamer	Rocket League	Online Friend & Roommate	N/A	N/A
8 (in person)	15	Female	Student	Psychology	Bystander	N/A	N/A	At Home	Roommate
	16	Female	Student	Psychology	Bystander	N/A	N/A	On Tennis Court	Sister
	17	Male	Student	CS	Bystander &Streamer	Teaching Coding	Family	At Friend's Home	Friend
	18	Male	Student	CS	Bystander &Streamer	Food	People in Restaurant	At Home	Roommate
	19	Female	Student	CS	Bystander	N/A	N/A	At Friend's Home	Friend
9 (in person)	21	Female	Student	Psychology	Bystander &Streamer	Teaching English	N/A	In Public	Friend
10 (in person)	22	Female	University Staff	Communication	Bystander &Streamer	Sport Game	Children	At Home	Children
11 (in person)	23	Male	Student	CS	Streamer	Sport Game	Public Bystanders	N/A	N/A
12 (online)	24	Male	Student	Game Design	Bystander &Streamer	Casual Game	N/A	At Home	Friend & Roommate
13 (online)	25	Female	Full-time Streamer	N/A	Bystander &Streamer	Singing &Dancing	Family	At Restaurant	Unknown Streamer