Do Streamers Care about Bystanders' Privacy?
An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management

YANLAI WU*, University of Central Florida, USA
XINNING GUI, Pennsylvania State University, USA
PAMELA J. WISNIEWSKI, Vanderbilt University, USA
YAO LI, University of Central Florida, USA

Live streaming has become a popular activity world-wide that has warranted research attention on its privacy related issues. For instance, bystanders' privacy, or the privacy of third-parties captured by streamers, has been increasingly studied as live streaming has become almost ubiquitous in both public and private spaces in many countries. While prior work has studied bystanders' privacy concerns, a gap exists in understanding how streamers consider bystanders' privacy and the steps they take (or do not take) to preserve it. Understanding streamers' considerations towards bystanders' privacy is vital because streamers are the ones who have direct control over whether and how bystanders' information is disclosed. To address this gap, we conducted an interview study with 25 Chinese streamers to understand their considerations and practices regarding bystanders' privacy in live streaming. We found that streamers cared about bystanders' privacy and evaluated possible privacy violations to bystanders from several perspectives. To protect bystanders from privacy violations, streamers primarily relied on technical, behavioral, and collaborative strategies. Our results also indicated that current streaming platforms lacked features that helped streamers seamlessly manage bystanders' privacy and involved bystanders into their privacy decision-making. Applying the theoretical lens of collective privacy management, we discuss implications for the design of live streaming systems to support streamers in protecting bystanders' privacy.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**.

Additional Key Words and Phrases: privacy, live streaming, bystander's privacy, collective privacy management

1 INTRODUCTION

Live streaming has risen to prominence as a new form of synchronous social media worldwide that allows users (i.e., live streamers) to share their lived experiences and interact with other users (i.e., viewers) in real-time from any location [65, 70]. For instance, Twitch is a popular gameplay-based live streaming platform in the US and has approximately 140 million monthly

Authors' addresses: Yanlai Wu, yanlaiwu@knights.ucf.edu, University of Central Florida, 4000 Central Florida Blvd, Orlando, Florida, USA, 32816; Xinning Gui, Pennsylvania State University, State College, Pennsylvania, USA, 16801; Pamela J. Wisniewski, Vanderbilt University, Nashville, Tennessee, USA, 37235; Yao Li, University of Central Florida, 4000 Central Florida Blvd, Orlando, Florida, USA, 32816, yao.li@ucf.edu.

127

active streamers [75]. DouYu, one of the biggest online live-streaming websites in China, reported 433.4 million registered users in 2021 [71]. Because of the ubiquity of live streaming, unintended privacy violations are emerging as a new and critically important societal problem in need of further examination. For instance, video game content creators on live streaming platforms in the U.S. often draw large audiences among young viewers, which could create concerns about Child Online Privacy Protection Act (COPPA) violations [52]. A Chinese live-streaming platform, Shuidi (Water Drop), which broadcasted footage from public venues such as restaurants and shops, was shut down due to concerns about violating people's privacy [81].

As streamers' webcam and microphone can easily capture individuals (i.e., bystanders) who are in the range of a proximal distance to the streamers [21], these types of privacy violations are becoming more commonplace. Bystanders in live streaming can be unknown passersby in the public spaces [21, 47], known people in the same household, such as family and roommates [43] and known or unknown virtual participants, such as in-game teammates [43]. Several studies have indicated that bystanders have privacy concerns about their personal information or inappropriate and/or embarrassing activities [15, 36, 64] being captured [15, 60, 64], stalked [78], and misinterpreted [21, 64] in sensitive locations, such as banks [17], bathrooms [78] and restaurants [64]. Such information leakage would cause a series of negative consequences to bystanders, including identity theft [9], financial loss [54], negative reputation [62], doxing [13] and harassment [9]. However, bystanders have little agency over their privacy given that the live streamer has direct control to share and moderate the bystanders' video and audio capture [43, 47, 64]. As such, bystanders' personal information, including their physical appearance, body movement, voice, and behaviors can be unintentionally disclosed by streamers to their audiences [21, 43, 47]. It is frequently reported in the news that streamers overly exposed their bystanders' personal information in live streaming, which violates bystanders' privacy and creates conflicts between bystanders and streamers [11, 53, 63].

While most prior literature has examined bystanders' privacy concerns from the perspective of bystanders (e.g., [5, 19, 21, 43, 47]), no research has investigated bystanders' privacy from streamers' points-of-view. As such, there is a lack of understanding as to how streamers perceive bystanders' privacy or what streamers do to protect bystanders' personal information. Understanding the streamers' considerations and actions towards bystanders' privacy is important because the existing live streaming platforms do not have any functionality for bystanders to manage their privacy. Therefore, only when streamers accurately evaluate bystanders' privacy expectations and are willing to take actions to preserve bystanders' privacy, could they efficiently protect bystanders' privacy from being violated. Our study aims to fill this gap and seek to answer the following research questions:

RQ1) *What considerations, if any, do live streamers make regarding bystanders' privacy?*
RQ2) *Given these considerations, what actions do live streamers take to preserve bystanders' privacy? Are these actions effective?*

To answer these research questions, we conducted 25 semi-structured interviews with DouYu streamers. We found that streamers indeed cared about their bystanders' privacy and considered different aspects, from their perceived bystanders' personalities to their perceived bystanders' information sensitivity, to decide whether bystanders' privacy was at risk and whether they should take actions to protect bystanders' privacy. However, streamers' considerations were largely based on their own assumptions, as bystanders were not fully included in the streamers' privacy decision-making. Streamers were willing to adopt strategies, especially technical, behavioral, and collaborative strategies with bystanders, to protect their bystanders from privacy violations during live streaming. However, these strategies might not work because current streaming platforms lack

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management
127:3

features that help streamers effectively communicate with bystanders about bystanders' privacy preferences in real time.

By examining live streamers' considerations and strategies for managing bystanders' privacy, the contributions of this paper to the Human-Computer Interaction (HCI), CSCW, and privacy research are three-fold: 1) We uncovered the challenges in collective privacy management under an understudied context - live streaming, where information sharing is synchronous and can expose rich personal information (audio and video) about the bystanders. We find that managing bystanders' privacy in real-time is much more challenging than in asynchronous information sharing. 2) This study advances the understanding of bystander's privacy challenges from a new perspective - streamer's perspective, who is a key stakeholder in controlling bystanders' exposure in live streaming. We find that streamers care about bystanders' privacy and proactively evaluate potential violations to bystanders' privacy from multiple perspectives; 3) We discuss the design implications on how to protect bystanders' privacy in live streaming, such as how to facilitate the mutual understanding of bystanders' privacy between streamers and bystanders and how to collectively address the real-time change of context for both streamers and bystanders, as there is little privacy protection mechanism for bystanders in current live streaming platforms.

2 A THEORETICAL LENS OF COLLECTIVE PRIVACY MANAGEMENT

Privacy researchers have long argued that privacy is an interpersonal process that sometimes moves beyond individual control [4]. For instance, Altman defined privacy as a dialectic interpersonal boundary regulation process [4]. In this process, people adjust their boundaries by restricting or seeking social interactions with others in order to achieve desired privacy over time. The emphasis on social interaction regulation makes privacy not limited to individual decisions but also includes the group-level coordination. As such, Petronio's theory of communication privacy management (CPM) extends Altman's theory by including the concept of multi-stakeholders in co-owned information sharing and highlighting that collaboration and coordination between the stakeholders is necessary [59]. Stakeholders in information sharing include all the parties [59], such as people who send the information, the people who receive the information, and those who may somehow be otherwise implicated in the sharing process. When a sender shares information with recipients, the recipients co-own the information, which turns the management of the information disclosure into a collective effort. All stakeholders need to develop and negotiate privacy norms collaboratively to coordinate each other's boundary expectations. This process determines what information is expected to be permeable/non-permeable, and to whom it is appropriate/inappropriate to disclose the information. However, different stakeholders may have different needs and understandings of privacy expectations based on demographics, motivation, context, personal background, and norms [59]. Hence, coordination might sometimes fail when stakeholders do not mutually reach an agreement or when they have different expectations regarding privacy management, which leads to boundary turbulence [59]. Boundary turbulence heightens stakeholders' privacy concerns and may prompt them to renegotiate their boundaries or even withdraw completely [14, 42].

In addition to Altman's and Petronio's theories, the tenet of Nissenbaum's contextual integrity (CI) also highlights interpersonal and group-level privacy management. Contextual integrity describes that people's privacy is based on norms of appropriateness in diverse contexts, each of which has its own set of expectations for who should send what personal information to whom in what specific occasions [32, 55]. Specifically, this framework recognizes several contextual elements that should be taken into account when defining privacy violations, including actors, information type, and transmission principles [32, 55]. Actors refer to the information subject (the subject of the information), sender (people who send the information) and recipient (people who receive the information). Information type means what type of information is disclosed, such as home

address, medical records and salary. Transmission principles are the rules of regulating the flow of the information from one actor to another [51, 55]. In most cases, a change in one element would cause the change of the context, which leads to the change of norms of appropriateness. Failing to consider the change of context would lead to privacy violations, as information which is appropriate in one context might be problematic in another context [56].

A shared theme across each of these three theories is the importance of collective perspectives in privacy management that cannot be studied from a single vantage point of one key stakeholder. This theme applies to the bystander's privacy issues in live streaming. First, the multi-stakeholder coordination in CPM happens in live streaming. In the context of live streaming, bystanders, such as streamers' family members, roommates, or people who are physically or virtually around the streamers, can be easily captured by the streamer's camera and microphone during live streaming [21, 43, 47]. Bystanders are no longer the only owners in their information sharing. Streamers become an important stakeholder who can decide on the information disclosure [32]. To achieve bystanders' desired privacy, streamers and bystanders need to negotiate the privacy norms. If the negotiation breaks down, i.e., streamers and bystanders have different interpretations of bystanders' privacy, boundary turbulence happens and bystanders' privacy cannot be achieved. Thus, a central requirement in the negotiation is to have streamers accurately understand bystanders' privacy norms. Second, CI is applied in live streaming as well. When no bystander is involved, streamers are both the information subjects and senders, and the audience are the recipients. But when bystanders are streamed, the information subject is changed to bystanders. Then the context changes. Information sharing that was appropriate between streamer and audience might no longer be appropriate when bystanders are involved. For example, streamers might be willing to disclose their physical appearances to attract their audience, but bystanders might have concerns with sharing their looks. In this way, it is necessary for stakeholders to correctly capture the change of context.

3 RELATED WORK ON BYSTANDER PRIVACY

In this section, we review previous research on bystanders' privacy issues in collaborative photo sharing on social media, collaborative video sharing and live streaming, as these research streams have all raised attention to bystanders' privacy concerns.

3.1 Collaborative Photo Sharing on Social Media

Based on Altman's privacy regulation theory, CPM and CI, researchers in the HCI community have examined bystanders' privacy management in diverse socio-technical contexts. One of the most widely studied context has been collaborative photo-sharing. Collaborative photo-sharing indicates the situation where users (i.e., senders) post photos online that reveal others' information [28, 29]. In collaborative photo sharing, the sender is the person who posts and manages photo sharing [8, 28]. In this case, bystanders would include individuals who are pictured, mentioned, linked or tagged other than the photo owner who shared the picture [14, 22]. Similar to the case of live streaming, bystanders in photo sharing on social media do not have direct control over the information disclosed about them online [49]. Thus, when information co-owners and bystanders have different privacy norms of photo-sharing, it might put the bystander's privacy at risk. For example, Lampinen et al. have shown that bystanders often have concerns about their inappropriate behavior, such as appearing drunk or undressed, being posted through group photos on Facebook [36]. Often, photo owners share such photos of bystanders because they felt the photos were harmless and fun [24]. To cope with bystanders' privacy concerns, owners could adopt both preventative and corrective strategies, such as grouping audience into distinct groups [35, 76], avoiding uploading photos with inappropriate content [38], untagging [14] and removing unwanted contents after

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management

127:5

negotiation [14, 36]. Bystanders could also self-censor the content of the photos [14], change their everyday offline behavior to satisfy photo sharing context [8] and discuss with the owner whether a group photo is appropriate or problematic to be posted on social media [14, 36].

3.2 Collaborative Video Sharing

Similar to collaborative photo-sharing, many video sharing technologies, such as lifelogging, wearable cameras, Augmented Reality (AR), drones, and Internet of Things (IoT) (e.g., smart home devices), have raised privacy concerns to bystanders as well, as shown in prior work on ubiquitous/pervasive video sharing [2, 3, 18, 33, 78]. We review this prior work because live streaming is also about video sharing. Ubiquitous/pervasive video sharing technologies can capture the images of bystanders when the owner is using the technology, but do not offer bystanders much control over their information exposure, nor a way for bystanders to negotiate with the owners about their privacy needs, thus raising significant privacy concerns to bystanders [21, 43, 64]. For example, bystanders in lifelogging are often worried about being misrepresented due to the partial capture [64] or being identified at a certain location engaged in certain activities in others' lifelogs, such as performing transactions on an ATM machine [60]. For AR, bystanders are worried about being captured in private places such as bathrooms, bedrooms and other people's homes [18].

However, different from collaborative photo-sharing, lifelogging, wearable cameras, AR, drones, and IoT are normally less visible than a camera and can capture a larger set of bystanders' personal information other than images, such as bystanders' voices and movements, both of which also happens in live streaming. Therefore, bystanders' privacy management would be more challenging in the video sharing contexts since bystanders are not fully aware of being recorded in most cases [21, 48, 50]. For example, bystanders in IoT devices are upset about being recorded by the smart speaker, such as their conversation when visiting a friend [37, 50], and being monitored through the security camera by the device owner, such as surveillance of nannies working in the employer's home [7]. Bystanders involved in others' usage of wearable glasses are concerned with being recorded in personal activities or in private spaces, such as having a meal in a restaurant [17, 64] or in the living room [15]. Bystanders in drones have concerns about being stalked, peeked at through the window, and recorded them doing private things, such as bathing at home [5] and shopping with close friends in a mall [78]. To solve the privacy issues of bystanders in video sharing, researchers highlight the necessity to notify and ask for permission from people near the devices [5, 19, 21, 50]. They have also proposed obscuring details of privacy-sensitive objects and replacing privacy-sensitive objects in videos with abstract cartoons taken from clip art [26], or applying activity-oriented partial obfuscation to preserve a specific type of hand-related activity while obfuscating everything else [3].

3.3 Bystanders' Privacy in Live Streaming

Compared with collaborative photo sharing, life logging, wearable cameras, AR, drones, and IoT, the bystanders' privacy challenges in live streaming have received limited research attention to date. To our best knowledge, only three studies have touched on or discussed bystander's privacy issues in the context of live streaming [21, 43, 47]. Lu et al. conducted a mixed methods study with viewers to understand outdoor live streaming practices in China [47]. They reported that viewers often saw the interactions between streamers and passersby in the outdoor live streaming [47]. Faklaris et al. investigated bystanders' privacy concerns in outdoor spaces through simulating the act of streaming live video using a mobile phone [21]. They found that bystanders were less aware of themselves being streamed in the context such as sports event compared to the meeting event. Bystanders wanted stronger notifications and precaution consent before being streamed [21]. Li et al. highlighted bystander's privacy issues in team-based video game live streaming who

were accidentally streamed by other players [43]. They found that gamers were concerned about their sensitive personal information, inappropriate self-presentation and group impression being streamed by others. Gamers would withhold sensitive information and collaborate/negotiate with the streamers to protect their personal information from being streamed.

A common theme among this literature was that it aimed to understand bystanders' privacy issues from the bystanders' perspective. No prior study pays attention to how streamers perceive their bystander's information disclosure and how they protect their bystander's privacy from being violated. It is important to examine streamers' considerations towards bystanders' privacy because bystanders have to rely on the streamers to protect their privacy. Prior work has pointed out that bystanders have little agency over their privacy, whereas streamers usually have direct control over the video and audio sharing [43, 47, 64]. Many popular streaming platforms, such as Twitch and DouYu, do not provide any mechanisms to let bystanders directly manage their privacy, nor allow bystanders to request streamers to protect their privacy. Thus, only when streamers are self-motivated to raise awareness and take actions can bystanders' privacy be protected. Currently, it is unknown whether, when and why streamers are willing to consider what to share and what not to share about the bystanders, and what actions they may take to protect bystanders' privacy. Our work fills this gap by examining the bystander's privacy concerns from the streamers' perspectives. We study how streamers consider bystanders' privacy, and what actions they would like to take to safeguard bystander's privacy. Our findings inform on how to motivate and technically facilitate streamers to better preserve bystanders' privacy.

4 A CASE STUDY OF DOUYU

In this section, we introduce our study site, DouYu. We chose DouYu as our study site mainly for two reasons. First, DouYu is not only widely used but also representative in the sense that it shares many privacy and streaming features with other popular live streaming platforms. Second, there has been several prior work showing that it is common on DouYu to involve bystanders in live streaming [46, 47], such as conversing with strangers on street, inviting teammates to stream jointly and streaming family and friends by accident. Although these studies do not touch upon either bystanders' privacy or streamers' considerations towards bystanders' privacy, they have shown that DouYu could be a suitable site to investigate bystander's privacy issues.

DouYu is one of the biggest online live streaming platforms in China which was founded in 2004 [82]. There is an estimate of more than 7 million unique viewers and 66 million page views of DouYu per day [82]. Though DouYu started as a game-centric live streaming platform, it now includes a diverse range of channels including gameplay, travelling, daily lives, talented performances and commercial events [79]. Streamers aim to create interesting content and attractive performances to engage their viewers, ranging from their life to game skills to outdoor activities to commercial events [77].

Similar with other popular live streaming platforms (e.g., Twitch, Facebook Live, etc.), DouYu streamers share their live performance through a webcam, a mic, and a computer/mobile device to run the streaming platform (Fig. 1). Through the webcam, streamers could share their facial expressions, appearance, body movements and performances with their viewers. The microphone allows streamers to explain about their performances, present their audio-based talented performances such as singing, and also chat with viewers. They can also share their screen to broadcast their computer contents to viewers.

Bystanders' information is exposed through these three channels as well. The webcam and microphone could also capture bystanders who are physically around, exposing their physical appearances, ongoing activities and voices. The screen sharing could disclose the information of bystanders who are virtually around, such as friends' messages and teammates' gameplay.
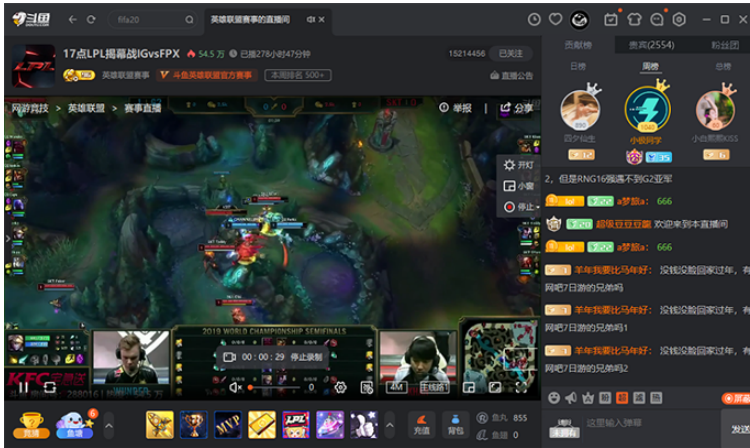
Fig. 1. Screenshot of DouYu live streaming from viewer's view

DouYu provided several features for streamers to control information disclosure. For example, DouYu streamers can enable/disable video/audio sharing, start/pause/stop streaming to decide what viewers can see and hear. Streamers can also apply beauty filters to enhance their physical attractiveness, set up a "virtual background" to hide real background, add an "overlay" (an image or texture) to block the unwanted information, and selectively manage sources of screen sharing/video/audio. Most of these features are also provided on other popular live streaming platforms, such as Twitch, YouTube Live and Facebook Live.

5 METHODS

5.1 Study Overview

We conducted 25 semi-structured interviews with DouYu streamers. The interview questions were designed to probe streamers' privacy considerations regarding their bystanders and actions to preserve bystander privacy. We started with questions about the content streamers have streamed, the length of their live streaming experience, the platform they used to stream, and their motivations to stream. We then asked about their live streaming environment, including the place they used to stream at, whether there were other people (bystanders) involved in the live streaming, and who were the bystanders. When asking about interviewees' bystanders, we followed the definitions of bystanders in prior work [21, 43, 47] and let interviewees broadly consider their bystanders captured in the live streams, including unknown passersby in public spaces, known people in the household (i.e., family, friends and roommates), and virtual bystanders (i.e., in-game teammates and contacts in an online conversation). We then put emphasis on probing in regard to bystanders' information disclosure and streamers' attitudes and practices about disclosing bystander's information, including what bystanders' information used to be streamed, any consequences due to the exposure, how streamers evaluated the sensitivity of their bystanders' information, and the strategies they adopted to prevent disclosing bystanders' information. The Appendix A contains the full interview questions.

Our participants included 15 males and 10 females. They were recruited through direct contact and word-of-mouth. We posted recruitment ads on both WeChat (the most frequently used social media in China) and Weibo (the most popular microblogging website in China), recruiting four participants and three participants respectively from these two platforms. We also asked participants who had been interviewed to help distribute the recruitment information, from which we recruited

#	Age	Gender	Occupation	Length of streaming	# Viewers	Topics	Bystander
1	27	Male	Student	5 times	5+	Mahjong	Roommate
2	28	Female	Student	3-4 years	300+	Warcraft, PlayerUnknown's Battlegrounds, Call of Duty	Family
3	23	Male	Student	15 days	30+	League of Legends PlayerUnknown's Battlegrounds	N/A
4	28	Male	Civil Servant	1 year	20+	JX3 (game)	Family
5	20	Female	Full-time Streamer	5 years	600+	Singing, Chatting Casual games	Family
6	22	Male	Freelancer	1 year	200+	Dota	Teammate
7	26	Male	Teacher	3 months	5+	Hearthstone	Family
8	25	Male	Student	2 years	80+	Hearthstone	Family
9	20	Female	Student	3 years	20,000+	Overwatch, PlayerUnknown's Battlegrounds	N/A
10	22	Male	Student	Half year	300+	Honor of Kings	Family
11	22	Female	Student	Half year	50+	Singing, Chatting	Boyfriend
12	18	Male	Crew	3-4 months	10,000+	Honor of Kings	Teammate
13	27	Female	Full-time Streamer	2 months	10+	Singing, Chatting	Delivery man
14	28	Male	Soft Engineer	1 month	8+	Singing, Gwent: The Witcher Card Game	N/A
15	23	Male	Student	3 months	1000+	League of Legends	Roommate
16	20	Male	Student	1 month	70,000+	PlayerUnknown's Battlegrounds, League of Legends	Teammate
17	30	Male	Entrepreneur	Half year	5+	Warcraft, PlayerUnknown's Battlegrounds, League of Legends	N/A
18	22	Female	Student	16 days	1000+	Chatting	Boyfriend
19	29	Male	Financial Analyst	1 year	10-20+	Hearthstone	N/A
20	23	Female	Student	2 months	10,000+	Apex Legends	Boyfriend, Family
21	29	Male	Computer Scientist	1.5 years	500+	Algorithm Teaching	Roommate
22	27	Male	Teacher	2 years	700+	Casual Games, Chatting, Outdoor Activities	Family, Friends
23	22	Female	Student	1 year	200+	Casual Games	Family, Teammate
24	20	Female	Full-time Streamer	2 years	1000+	Casual Games	Roommate
25	26	Female	Full-time Streamer	1 year	3000+	Singing, Chatting, Casual Games	Family, Teammate

Table 1. Demographics of interviewees

18 participants. By the time the researchers agreed that "theoretical saturation" [67] had been reached, 25 participants had been interviewed in total. This sample size is also in accordance with the typical sample size of interview studies in HCI [12]. All the recruited participants were at least 18 years old, had experience in live streaming, and are Chinese. Since the focus of this study is on streamers' attitudes to their bystanders' privacy, we intentionally recruited streamers with various occupational backgrounds, lengths of streaming, and numbers of viewers to have a better understanding of diverse streamers' perspectives. The participants we recruited included both full-time and part-time streamers, those who have been streaming for a few days to several years, and streamers who have just a few viewers to those who have tens of thousands. The demographic information of interviewees is presented in Table 1. 40% of our interviewees are female and 52% are between 18-24, which is in line with the demographics of the Chinese streamer population shown in the prior survey [1].

20 participants reported that they had bystanders while streaming. The most frequent types of bystanders are family, friends, partners, and roommates. Five participants did not have bystanders while streaming. We did not include them in our data analysis. We paid 70 CNY (about 10 dollars) for each participant through WeChat Red Pocket (a money transfer function on WeChat). The Institutional Review Board (IRB) approval was obtained from the university prior to study commencement and our participants were informed of the research purpose and procedure before being interviewed. Each interview was around 30 to 60 minutes. We audio-recorded the interviews using a digital voice recorder for transcription purposes, with oral consent from the interviewees at the beginning of each interview. To protect our interviewees' privacy, we deleted all the audio recordings after transcribing the interviews and anonymized interviewees' identifiable details.

5.2 Data Analysis Approach

We analyzed the interview data using thematic analysis [10] in an inductive approach. Three of the authors, who have expertise in live streaming and privacy research, participated in the data analysis. We first read the data to familiarize ourselves with the data and individually noted down the initial codes related to bystanders' information disclosure and streamers' attitudes and practices about bystanders' information disclosure. Then we compared our initial codes and grouped them into a combined list through rounds of discussions, which led to 73 codes. Building on the initial coding, we advanced our analysis to generate the overarching themes from our codes after extensive discussions. We also went back and forth between the themes and the dataset to collate codes into potential themes and sub-themes. The final thematic map consists of two primary themes: streamers' considerations towards bystanders' privacy and strategies adopted by streamers and bystanders to protect bystanders' privacy. The codes and themes can be found in the Appendix B. When reporting the data in the paper, we translated all the participants' quotes into English. To protect our participants' privacy, we used P1, P2, etc. to denote different participants.

6 STREAMERS' CONSIDERATIONS TOWARDS BYSTANDERS' PRIVACY (RQ1)

We found that most streamer participants cared about their bystanders' privacy, had different considerations towards their bystanders' privacy during their live streaming, and elaborated various rationales behind their attitudes. We categorized them into three types in the following section.

6.1 Based on Perceived Information Sensitivity

The sensitivity of the information about the bystanders involved was an important factor that streamers considered when evaluating whether their streaming behavior would violate bystanders' privacy. The evaluation of sensitivity relied on the identifiability of the information and potential privacy consequences of information disclosure. The bystander's personal information that our participants considered as sensitive included family matter, social relationship, physical appearance, occupation, and identifiable information (e.g., name, address, etc.). 6 out of 25 streamers believed disclosing such sensitive information might lead to negative consequences, such as being identified in real life, harassment, and cyberbullying, to bystanders. Hence, streamers were cautious about bystanders' sensitive information being accidentally disclosed in their live streaming. For example, P4 (male, 28) told us:

> I don't use webcam, cuz I sit with my wife while streaming and she always wears pajamas... Her voice is fine cuz voice is nothing personal. My audience can hear her all the time so it isn't a big deal. They get used to it. My wife and I often talk about why we lose the game and she often gives me advice on how to improve. For me, voice isn't something sensitive but photos and looks are cuz voice doesn't bring any bad consequences to my life. And what we talk about in streams is quite normal.

P4 based his evaluation on his criteria of what sensitive information was and whether the information disclosure would cause negative consequences to the bystanders. In P4's view, his wife's physical appearance, such as looks and figures, was sensitive because he believed this was identifiable information. However, his wife's voice was not sensitive for him because he believed that voice itself was not identifiable. Furthermore, his wife talked about games only, so the topic was not sensitive either. It would not cause any trouble to his wife in real life.

In addition to privacy consequences to bystanders, streamers also considered the consequences to themselves when evaluating information sensitivity. Disclosing bystander's sensitive information would sometimes negatively influence streamers themselves, such as losing attractiveness and being banned from the streaming platform. For example, P25 (female, 26) reported:

> I heard a famous streamer was banned (on DouYu) because a girl showed up with only a panty when he streamed. The audience was shocked and someone tried to notify the streamer about it. But the streamer didn't notice that. It happened so fast, just in a few seconds. Then the streamer was banned. He had to appeal. He couldn't cash out his revenue for like a month. Some people doxed that girl. She turned out to be a friend of the streamer. People blamed her for bringing this trouble to this streamer. That's why I tell my brother not go topless when he's streamed in my channel no matter how hot it is.

P25 evaluated the sensitivity of her brother's information based on not only the negative consequences to the bystanders, but also to the streamer themselves. She learned that disclosing bystander's sensitive information could make bystanders identifiable offline. More importantly, it would also negatively influence her live performance, as some of the sensitive information was inappropriate and would violate the code of conduct on the live streaming platform. For instance, streamers would be banned and fined by the platform for disclosing inappropriate information, regardless whether the information was about the streamers or the bystanders. Thus, P25 regulated her brother's dressing during streaming to prevent disclosing her brother's inappropriate information in her streams. Streamers might be more aware of the bystanders' sensitive information disclosure if it would have a negative impact on streamers themselves.

Voice (the way people produce sound), pseudonyms, nicknames, casual chat, and daily life were not perceived as sensitive information by 8 out of 25 participants because they were not considered to be identifiable nor would adversely affect bystanders' lives. Instead, such information disclosure would help streamers attract audience, as they could trigger interesting discussions between streamers and audience and make the streamed content more entertaining. For example, P15 told us that he found it entertaining when his casual chat with his roommate was broadcast as "many streamers would broadcast what they talk about with bystanders because audience can know more about the streamers". P23 (female, 22) also said:

> My audience could sometimes hear my mom call me to eat or my mom talks with my puppy. The audience found it lovely. They were like "go eat your meal" or "the dog is like you". I think it's ok to share it (mom's talk) in streams cuz I don't see any problem. It's just normal daily stuff. I like audience say my puppy is cute. I like they say my family is nice... My parents don't seem to have an issue with that. My mom was a little shy when she knew it. But she told me not to have too much connections with my audience in real life. She has some safety concerns, like how different it is between online and offline. You don't know who you are talking to online.

P15's and P23's stories to some degree indicated a discrepancy between how streamers and bystanders perceived the sensitivity of bystanders' personal information. P15 and P23 believed that trivial details about bystanders, such as daily stuff and casual talk, were not sensitive personal information because such information would not have any negative impact on either the bystander or the streamer. Instead, P15 and P23 found that such information disclosure could improve the attractiveness of their streams and promote their interactions with audience. However, P23's mother had expressed concerns that it was risky to disclose too many personal details to the unknown online audience. Her mom believed most people on the Internet were not as trustworthy as people in the real world. Disclosing too much personal information to the unknown audience would cause safety issues and other uncertainty. Therefore, there was tension between the streamer's and the bystander's perceptions of sensitive information.

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management

127:11

6.2 Based on Perceived Bystander's Personality

Streamers also perceived their long-term beliefs of the bystanders' personalities as another important factor when they evaluated bystanders' privacy. 3 out of 25 participants evaluated their bystanders' privacy based on their perceived personalities of their bystanders. Note that the personality mentioned by the interviewees was a simplified mental model based on their subjective perceptions, rather than the real personality of the bystanders which was objectively validated through personality tests (e.g., Big Five Personality Test [23]). Participants were able to perceive bystanders' personalities when they had a close relationship and long-term interactions with bystanders. Such long-term close interactions between streamers and bystanders shaped the streamer's perception of bystander's personality which would further drive the streamers to form their attitudes towards the bystanders' privacy. Based on our interviews, not all types of bystanders' personalities would affect streamers' evaluation of bystander's privacy. Their evaluation was mainly dependent on whether the bystander was perceived to be introverted or extroverted. Streamers believed that bystanders who had extroverted personalities were more willing to express themselves through information disclosure, so it would not be inappropriate for streamers to disclose extroverted bystanders' information to audiences. On the other hand, streamers believed bystanders who had introverted personalities were mostly reluctant to express themselves and shared about themselves in live streaming. Therefore, streamers would be careful about involving introverted bystanders in their live streaming. For example, P22 (male, 27) told us:

> I guess it has something to do with personalities. I have two friends since high school. One is pretty introverted. When he's streamed, he doesn't talk much. He is an excellent gamer. We asked him to stream games cuz he can easily beat those famous game streamers. But he doesn't want to stream. He's very indoorsy and isn't really good at expressing himself. When he sometimes got involved in my streams, he was impacted, but not very seriously, since we are very close. He won't ask me to stop, like 'hey you stop streaming'. He won't do that. The other friend is super outgoing. He lives pretty close to me so we often hang out together. He extremely loves to be on camera. Whenever I tell him he is streamed, he'll go out of his way to pose differently. Different friends have different personalities. What I can do is to respect them.

P22 decided whether to involve his friends in streaming based on whether his friends were introverted and extroverted. P22 understood that his introverted friend tended to be more quiet, reserved, and introspective and his extroverted friend was more talkative, sociable, and expressive. Therefore, he would stream more about his extroverted friend in his streams than his introverted friend. Such differentiation required a long-term interaction between the streamers and the bystander since P22 and the bystanders were high school friends and they lived close to each other. Moreover, such evaluation also required streamer's empathy and compassion to a large extent. In this case, he strongly cared about his friends' feelings and respect their needs, which resulted in his different attitudes and practices in disclosing bystanders' information in the live streams. However, as most introverted bystanders seldom explicitly expressed their feelings (i.e., P22's introverted friend would not directly ask P22 to stop streaming), they might be vulnerable if the streamers were not close or empathetic. Thus, it would be challenging for streamers to know introverted bystanders' privacy need.

"Camera shyness" is another personality that would affect streamers' evaluation of bystanders' privacy. Camera shyness is the inclination to avoid being photographed or filmed [16]. From long-term real-world interactions with the bystanders, streamers found that some bystanders were always reluctant to be on camera or felt awkward when being photographed. Streamers would try to avoid such bystanders being captured on camera in their live streaming in order to

respect bystanders' personality and protect their privacy of physical appearance. As P20 (female, 23) reported:

> I don't like my mom and my boyfriend showing up in my streams. They don't like being captured either. We all feel it's pretty awkward standing in front of the camera. It's weird, like we are being watched.

In this case, P20 protected her mom and boyfriend from being captured in her live streaming. She understood her mom and boyfriend's reluctance to be photographed from everyday interactions. More than respecting bystanders' personalities, such protection stemmed from the streamer's instinct to care about her family and the one she loved.

6.3 Based on Perceived Reaction from Bystanders

Streamers evaluated bystanders' privacy based on the in-the-moment reaction from bystanders. 5 out of 25 participants reported that they adjusted their attitudes and practices about disclosing bystanders' information based on bystanders' reactions at the moment of live streaming. They observed in real time that their bystanders would often verbally ask for confirmation about whether the live streaming was in progress (P10, P22) and whether the microphone and the webcam were on (P4, P24), as well as displaying an embarrassing facial expression (P10, P21, P24), dodging the camera (P22) or hastily completing tasks to minimize their exposure in live streaming (P24). When streamers noticed these reactions from their bystanders, they would realize their bystanders' concerns and take certain actions to protect their bystander's privacy. 2 out of 25 participants additionally mentioned that their female bystanders would commonly have such reactions when they (female bystanders) did not want to disclose their (female bystanders) unsatisfying appearances, such as no-makeup faces and casual clothes during live streaming. This was because disclosing such information might negatively impact their (female bystanders) persona. For example, P22's mom would check if the streamer used beauty filters when she was streamed in live streaming. P24's roommate would verbally check with P24 if her (the roommate's) face and clothing were broadcast in the streams.

> One of my roommates cares about her look a lot. She often says she doesn't want to be streamed without make-up. So she always asks me if I turn on the camera. When she knew she was streamed, she'd rush through activities at hand to reduce the exposure time in live streaming. She would walk around freely in the house only after knowing I turn off the camera (when she doesn't wear makeup). I think it's because she needs to be pretty all the time even if she only shows a second in my camera.

When streamers saw that their bystanders act the same as usual, they believed that the bystanders did not mind being streamed in live streaming. For instance, the bystanders talked or behaved as the way they would do when the live streaming was off, without any restrictions, even after they realized that they were being streamed. After streamers saw such reactions, they would reduce the impulse to protect bystanders' privacy based on the bystanders' reactions, even though streamers might sometimes be concerned that such information disclosure would violate bystanders' privacy. For example, P22 (male, 27) reported:

> While I'm streaming games, my friend can be heard in streams. We audio chat with each other, so my audience could hear what he says. He knows it. Our discussions were very private but he didn't seem to mind at all. We talked a lot about his wife, their daily life, their plans, like "time to go to bed" and "plan to have a baby". We also have lots of guy talks, like pretty girls, friends who got divorced or others' new relationships. He likes chatting about these topics even if he knows I'm streaming. Well, if he's ok with sharing these, I'm ok too.

In this quote, P22 evaluated his friend's privacy based on the friend's reaction rather than his own perception of the sensitivity of the information. P22's friend mentioned lots of his own personal information and others' personal information in live streaming. P22 believed such contents were sensitive. He thought that his friend would be mindful when disclosing such information to the audience. However, his friend insisted on sharing information without any hesitation. His friend's reaction changed P22's attitude towards his friend's privacy in live streaming. He did not take any action to prevent disclosing the friend's information that he used to perceive as sensitive during live streaming.

7 STRATEGIES FOR PRESERVING BYSTANDER PRIVACY (RQ2)

To prevent bystanders from privacy violations in live streaming, streamers applied strategies to manage bystanders' information disclosure. In some situations, bystanders' privacy could be protected via streamers' individual efforts, while in other situations, the privacy strategies could not be implemented only by the streamers, but required streamers and bystanders to collaborate. As such, the strategies could be grouped into two categories: streamers' individual efforts and collaborative strategies. This grouping was in line with the theoretical lens of collective privacy management.

7.1 Streamers Took Individual Efforts to Protect Bystanders

Several streamers in our interviews proactively developed their own strategies to protect their bystanders' privacy. These individual-level strategies do not require coordination between streamers and bystanders. The streamers take the responsibility to implement these strategies. These strategies rely on either technical and behavioral effort. Technical strategies are supported by features in software and hardware inside and outside the live streaming platform. By contrast, behavioral strategies are related to streamers' behaviors.

7.1.1 Streamers Developed Technical Strategies to Protect Bystanders' Privacy. 10 out of 25 participants, ranging from beginner streamers to experienced streamers, reported that they would rely on technical strategies, such as disabling the video/audio feeds on the live streaming platforms, or turning off their headsets and webcams to avoid exposing bystanders' physical appearance and conversation to the audience. Among these ten participants, eight of them reported that they adjusted microphones and webcams during live streaming when they realized bystanders were involved in their live streams. For example, P2 (female, 28) reported:

> I was living alone but now I live with my brother. He doesn't come to my room very often. But he sometimes might call me during my streaming. When he called me, I turned off the mic immediately. There is a button on the platform to mute... I think casual talks are ok, like what to eat and daily stuff. But family matters are not ok.

In addition, 3 out of 25 participants, who had at least one and a half years' live streaming experience and a considerable number of viewers, also mentioned that they would upgrade their streaming equipment to reduce the ambient sound, including the bystander's voice. For example, P21 (male, 29) said:

> Once I was streaming, my roommates came back from zoo. They were very excited and talking about the animals. Although they were talking very loudly, they were far away from my mic. Also, I upgraded my equipment recently to reduce the background noises and improve the audio quality.

Most streamers felt these technical strategies were convenient and effective for preventing bystander's information disclosure. For example, P23 (female, 22) said,

It's very easy to control the bystander's voice. You only need to press the on/off button on the platform, that's it.

However, these features are mostly all or nothing. Once streamers turned off the video/audio sharing, their own information sharing was stopped in addition to bystanders'. Streamers could not selectively share video and audio using these features. Therefore, disabling the video/audio feeds might sometimes have a negative impact on the streamer's performance, as it would also shut down streamers' information disclosure, which was an important component in streamers' live performance. For example, P24 (female, 20) said:

I streamed at home at that time. I was afraid my parents would walk around and show up in the camera, so I turned off the webcam... But streamers turn on the webcam to attract more audiences and make their streaming more interesting. I also want to engage my audiences and have more audiences, right? You can see big streamers all show their faces in streams. No one will watch a streamer who doesn't show the face. If I don't turn on the webcam, my audience will ask me why I turn it off.

This participant disabled the camera before live streaming when he streamed at home to protect his family from being streamed at the cost of sacrificing his performance. He indicated that it was important for streamers to disclose looks to attract more audience and make streaming more engaging because audience preferred to watch streamers who disclosed their physical appearances. His audience would ask him to turn on webcam if he did not. However, he highly valued his family's privacy so he chose to protect his family by turning off the webcam even though such behavior would negatively affect his performance. Therefore, streamers had to balance between their own performance and their bystanders' privacy during live streaming.

7.1.2 Streamers Applied Non-technical Behavioral Strategies to Protect Bystanders' Privacy. Aside from technical strategies, 6 out of 25 streamers also used behavioral strategies, such as scheduling streaming when bystanders were not around, and adjusting their streaming environment in advance to avoid disclosing bystander's information. For instance, P10 and P23 would arrange their streaming when their parents were not at home. P13 would avoid ordering deliveries to avoid the deliveryman being streamed. P18 and P20 would use the wall as their background to prevent bystanders passing by. P21 and P23 would close their door to reduce the chance of disclosing their bystander's information.

However, behavioral strategies sometimes were in a conflict with streamers' desired streaming quality and comfortable environment. Streamers typically wanted to stream with good lighting to elevate their looks, and with a strong WiFi connection to ensure a nice viewing experience for audience. Some streamers, such as P10, wanted to stream in a comfortable environment. Streamers might trade off bystanders' privacy for higher streaming quality and more comfortable environment. For example, P8 (male, 25) mentioned that his parents had been streamed when he streamed at home. When asked why he did not choose to close the room door to prevent his parents from showing up in his stream, he explained:

I streamed at living room at that time. Because living room had better light and internet. My parents had to be streamed when they walked around in the living room.

Another participant, P5 (female, 20), mentioned another reason for not adopting behavioral strategies, such as closing the room door. She believed that it might negatively affect her family relationship:

I have a stepbrother. I just can't lock the door during streaming to avoid my brother coming in cuz that'll affect our relationship.

7.2 Streamers and Bystanders Collaborated on Privacy Management

Participants commonly reported that they would collaborate with their bystanders to protect bystanders' privacy. Different from streamers' individual strategies, collaborative strategies were adopted when streamers and bystanders both wanted to protect bystanders' information in live streaming. Such strategies were either led by streamers, by bystanders or via the mutually agreed norms between streamers and bystanders.

7.2.1 Collaborative Strategies Led by Streamers. Streamers would verbally communicate with bystanders and ask for their cooperations to prevent bystanders' information from being disclosed. 4 out of 25 participants reported that they would verbally notify their bystanders in advance about the upcoming live streaming and the hardware devices they were going to use. In this way, bystanders could know beforehand which kind of personal information would likely be revealed so that they could coordinate accordingly and take appropriate actions to protect their privacy, such as lowering their voices, stopping talking, and using lip-synching to mute voices. Such collaboration between streamers and bystanders was usually initiated by the streamers, and could not be successful without bystanders' cooperations. Participants who used such strategies had between a few days to 1 year of streaming experience. For instance, P5 would ask her little brother not to mention name, age, birthday and address in live streams since he had no idea of the negative consequences brought by his involvement. P11 and P18 would tell their boyfriends that their streaming was about to start before each broadcasting so that their boyfriends would stop talking after being notified. Such communicative strategies were mostly preventive and requires agreement between the streamers and the bystanders on information disclosure.

Apart from these preventive collaboration strategies, another 4 out of 25 participants, whose live streaming experience ranged from 3 months to 5 years, reported that they would immediately inform their bystanders in the moment that they (bystanders) were about to disclose potentially private information during the live stream. These streamers were even more sensitive to privacy violations than the bystanders. They could notice the upcoming dangerous information disclosure from the bystanders before the bystanders themselves realized. They would proactively warn the bystanders about it and asked bystanders to stop their disclosure activities. Once receiving the streamer's warnings, bystanders would stop their activities accordingly. For example, P24 (female, 20):

> My two roommates and I share a balcony. When they go to the balcony, they or part of their outfit will show up in the streams. The audience would be like "hey your roommate's shoes were there" or "whose shoes". But the other days, because of the (exposed) outfit, someone recognized us (me and my roommate) when we shopped drinks. Since then, I warned my roommates every time when they were about to show up. I just told them "my camera is on, don't come" or "wait a second, let me turn off the webcam and mic". Other than that (warning), I don't think there are any good ways to prevent them from showing up in my streams. Frankly speaking, all I can do is to let them be more aware. They might have emergencies that they have to speak, like picking up deliveries. You can't just keep them silent all the time.

P24's strategy was to actively remind her roommates during the streaming about the potential exposure of their apparel through the webcam. Since they had been recognized in real life, P24 was quite sensitive to exposing her roommates' information. However, her strategies required her to continuously communicate with her roommates in the mid of the streaming, and required her roommates to continuously collaborate, which was a significant burden to both of them. P24 also mentioned the flaws of such strategies, as it was impossible to ask her roommate to collaborate

all the time. Bystanders had their own life and had to disclose personal information when needed. This indicated that privacy strategies might fail because streamers' streaming need and bystanders' personal need could not always work with each other.

7.2.2 Collaborative Strategies Led by Bystanders.
Streamers also noticed that bystanders sometimes had to interrupt the live streaming when they had urgent issues to discuss with the streamers, such as, asking the streamer to eat dinner and family matters. 3 out of 25 participants with half-year to 2-year live streaming experience reported that their bystanders had led collaborative strategies to protect their information from being disclosed. To avoid interrupting the broadcasting and disclosing their unwanted information, bystanders would initiate collaborative strategies, most of the time non-verbally, to ask streamers to coordinate accordingly. In such collaboration, bystanders usually knew that the broadcasting was in process. Thus, they wanted to send a signal to the streamers to express their need to communicate with streamers but also wanted to withhold their personal information from the audience. Thus, they would lower their voice, lip-synching, pat on the streamer's shoulder and gently knock on the wall or desk, to let the streamers know they had the need to talk and they did not want to disclose physical appearance, conversation content, and casual attire to the audience. After receiving the signal from bystanders, streamers would realize that their bystanders were not willing to get involved in the streaming so that they would disable speakers and webcams to protect their bystanders' privacy collaboratively. For example, p4 (male, 28):

> For example, if my wife wants to discuss about the games with me, she'll ask me if the speaker is disabled. I'll double-check the speaker. We'll start our discussion after the speaker is turned off.

7.2.3 Mutually Agreed Norms.
Norms on preserving bystanders' privacy were shaped naturally based on the mutual goal of streamer and bystander, that is, to protect bystander's information from being disclosed during live streaming. Unlike the previously mentioned collaborative strategies led by streamers and bystanders, streamers and bystanders equally participated in establishing and complying with shared norms. They did not need to remind each other constantly about what could be shared and what not during live streaming.

3 out of 25 participants, P20 (female, 23), P24 (female, 20) and P25 (female, 26), described that they established shared norms regarding bystanders' privacy during living streams. Two of them (P24 and P25) had the experience of sharing norms with bystanders who were in virtual space. The interactions between virtual bystanders and streamers were usually part of the streaming performance. To make streaming more engaging, streamers would sometimes invite their friends to co-stream with them. These bystanders did not need to be physically around streamers to broadcast but they would audio chat with streamers and their voices would be disclosed during live streaming. With the norms in mind, once the live streaming started, both streamers and their virtual bystanders would focus on the streaming content only and not mention any topics related to bystanders' personal information in live streaming. For example, P24 (female, 20):

> Most of my friends are also streamers. We often audio chat in-game while I'm streaming. Once I say the streaming starts, they know immediately what to say and not to say. We have been friends for a long time. We know each other's personal information, like name, phone number. We're very careful not to reveal these information, like we don't talk about these in streams, we only focus on games. We won't say "I know a popular restaurant that nears your home on xxx street". Instead, we say "I know a popular restaurant nearby".

Because P24 and her friends were both streamers, they established shared norms that avoiding talking about personal information in live streaming. The norms were established implicitly without much explanation from either the streamer or bystander side. Most of P24's friends were also streamers so they had a clear agreement on the negative consequences of information exposure. The knowledge of live streaming made them understand immediately what they should disclose and what they should not disclose during live streaming. Hence, they only talked about game-related content and avoided disclosing each other's personal information in live streaming.

Apart from bystanders who were in virtual space, bystanders who were in physical space would also develop norms with streamers to minimize personal information disclosure. Different streamers might share norms with their bystanders in different ways in physical space. For example, P20 (female, 23) communicated with her boyfriend through eye contact during live streaming and they also took advantage of the third-party app to communicate with each other when she was broadcasting. P24 (female, 20) and her roommates used nicknames during her live streaming to deter revealing real names. P25 (female, 26) and her brother also spoke with each other using dialect which could only be understood by a few people.

8 DISCUSSION

In this paper, we explored streamers' privacy considerations and strategies regarding their bystanders' information leakage during live streaming. While most previous work investigated bystanders' privacy concerns from bystanders' own perspectives, our paper is among the first to look into bystanders' privacy from streamers' point of view in live streaming. Through an in-depth interview study with 25 streamers, we found how streamers evaluate their bystanders' privacy, the rationale behind the evaluations and how they preserve bystanders' privacy. Our findings showed that most streamers cared about bystanders' privacy and proactively protected bystanders from privacy violations based on their own understandings of bystanders' privacy need. Streamers were willing to individually and collaboratively adopt strategies to protect bystander's privacy from being violated. They applied technical and behavioral strategies, and worked with bystanders to safeguard bystanders' privacy. However, some of the strategies might fail when streamers and bystanders have different understandings of bystanders' privacy need, and when streamers have to trade off between their performance attractiveness and bystanders' privacy. We discuss the implications and contributions of these findings in the following subsections.

8.1 Challenges in the Two-Way Privacy Negotiation Between Streamers and Bystanders

First, our findings on streamers' perspectives in managing bystanders' privacy in live streaming shed light on the motives and rationales for the information senders to proactively perform collective privacy management and thus broaden the literature on collective privacy management [14, 66]. This is also one aspect that our work differs from prior work on bystanders' privacy management in live streaming. Prior studies on bystanders' privacy are mostly from bystanders' perspectives. To bystanders, they are concerned with certain personal information being disclosed by others in live streaming. For instance, Li et al. found that bystanders (streamers' teammates) had concerns about identifiable information, such as school name, address, and full name, as well as family issues and unsatisfying self-presentation to be streamed [43]. Faklaris et al. showed that bystanders were unwilling to have their images being streamed since they would be manipulated by audience and harm bystanders' public images and social relationships [21]. Lu et al. found that bystanders might easily forget their actions and behaviors were being broadcasted outdoors which would make them become a meme, virally famous or stalked online or in person [47]. Our study is different from this prior work, as we investigated bystanders' privacy from the streamers' perspective. How streamers think of bystanders' privacy is important because if streamers do not care about

bystanders' privacy, or streamers think differently from bystanders about what is inappropriate to share about bystanders, bystanders' privacy is highly likely to be at risk.

Then what are streamers' considerations of bystanders' privacy in live streaming? Our findings show that streamers indeed care about bystanders' privacy, but they made many subjective assumptions on bystanders' privacy preferences. For instance, P1, P2, P4, P23, P24, and P25 perceived bystanders' name, image, address, occupation, family matter and social relationship as sensitive information, as they believed disclosing such information would cause negative privacy consequences, such as stalking, harassment and cyberbullying. In contrast, bystanders' voice (the way people sound), casual chat, and inappropriate language were believed as non-sensitive information by six streamers, because that such information was non-identifiable and had been commonly shared in live streaming. Several interviewees, such as P10, P15, P20, and P23 would even intendedly share bystanders' voice and chat because they wanted to enrich their streaming content and make their streams more entertaining. In streamers' assumption of bystanders' personalities, streamers, such as P22 and P25, assumed that extroverted bystanders were more willing to share about themselves than introverted bystanders.

Are these assumptions valid? According to Communication Privacy Management (CPM), when an individual's personal information is shared, all the stakeholders, including data senders, subjects and recipients, need to negotiate with each other to reach agreement on what should be shared with whom [59]. Without effective negotiation, agreement fails and boundary turbulence happens, which would raise privacy issues to stakeholder [59]. However, we found that for all their assumptions, streamers did not check with their bystanders. The privacy negotiations between streamers and bystanders is mostly one-way that are largely based on streamers' own assumptions without communicating with the bystanders, which is contrary to the two-way negotiation suggested in CPM [59]. In our study, it is unknown whether the bystanders believed their voice, casual chat, and inappropriate language was non-sensitive, whether the bystanders agreed with the personality profiling by the streamers and whether bystanders truly did not mind being streamed even if they were indeed extroverted. Bystanders might be sensitive about their voice, casual chat, and inappropriate language. For instance, Li et al.'s work showed that bystanders were worried about being misinterpreted by others through their voices and talks [43]. Faklaris et al.'s work showed that bystanders were concerned about their voices would be misrepresented by the audience which might harm bystanders' social relationships [21]. While it is unknown whether the bystanders of the streamers in our study are also concerned with voice, casual chat, and inappropriate language, the different perceptions around the sensitivity of voice, casual chat, and inappropriate language might exist and trigger boundary turbulence between streamers and bystanders. Additionally, streamers' assumption that bystanders who they perceived as extroverted people did not mind being streamed might also be disagreed by bystanders. For example, Bansal et al. indicated that extroverted people would have privacy concerns when talking about financial information [6]. Junglas et al. showed that there was no relationship between the personality trait of extraversion and privacy concern. [30]. Thus, despite that streamers care about bystanders' privacy in live streaming, the mutual privacy negotiation is not well established between streamers and bystanders. Thus, the streamers' considerations can be inconsistent with the bystander's privacy needs, and bystanders' privacy might be still at risk.

Admittedly, there are certain scenarios that two-way negotiation happens. For instance, when streamers consider bystanders' real-time reactions during live streaming, it is indeed two-way interaction, as bystanders is part of the privacy decision-making and both the streamers and the bystanders could receive the real-time feedback from each other about what not to share. Streamers mentioned several effective bystanders' verbal and nonverbal reactions, such as patting on the streamer's shoulder, gently knocking on the wall or desk, lip-synching, lowering voice, and asking

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management
127:19

for confirmation about whether the live streaming was in progress and whether the microphone and the webcam were on. These strategies allowed in-time coordination between bystanders and streamers in the privacy decision-making.

However, our findings uncover that there are challenges hindering the effective two-way privacy negotiation, a key component in CPM [59], in real-time information sharing. Specifically, streamers face two challenges in taking bystanders' in-the-moment reactions as the criteria to decide whether or not to stream bystanders: First, streamers might only be able to notice the bystanders' reactions when the bystanders were already involved in the streams. For example, P10 noticed his father's embarrassing facial expression after her father's voice was disclosed in streaming. P24 realized that her roommate's embarrassment after her roommate's outfit was disclosed during streaming. In these cases, although the bystanders indicated their reactions, part of bystanders' personal information had already been exposed.

Second, some bystanders might not want to explicitly express their privacy reactions to streamers because it might be offensive and impolite. For instance, P22 reported that his bystanders would choose to get away from the camera instead of directly expressing their concerns to him when he streamed playing basketball outside because it would be impolite for a bystander to come directly to a streamer to complain about being streamed. Prior work also found that most bystanders did not explicitly express their privacy concerns and mainly coped with privacy violations on their own efforts [21, 43]. Thus, if the bystanders choose to hide their in-the-moment reactions when being streamed, streamers cannot effectively evaluate what not to share about the bystanders.

Therefore, without the communication and confirmation with bystanders, it is unknown whether streamers' privacy considerations are effective and in line with bystanders' privacy preferences. Only when streamers sufficiently involve bystanders into their privacy decision-making, i.e., asking bystanders' what information they think sensitive and getting bystanders' reactions on what not to share, can streamers and bystanders achieve mutual agreement on bystanders' privacy. This indicates that there calls for sociotechnical interventions to facilitate streamers to confirm their assumptions with bystanders and involve bystanders into their privacy decision-making, as well as mechanisms to help bystanders express their privacy concerns, which is further explained in the "Design Implication" section.

8.2 Challenges in Addressing the Change of Context

Our study also reveal the challenges to achieve Contextual Integrity (CI) when bystanders were live streamed. Our findings show that achieving CI needs to be a collective effort for both streamers and bystanders in live streaming. CI defined privacy as appropriate information flows based on the context-specific norms [55]. The context is characterized by three parameters, actors (subject, sender, recipient), information type, and transmission principles. A change to one parameter would cause a change in the context, leading to the change of appropriateness of the information flow. Failure to recognize the change of context will result in privacy violations, as information flow that is appropriate in one context might be problematic in another [56]. Most privacy research and design that support CI focus on how to enhance individual effort to handle the change of context, such as notifying users of the change of context [45] and recommending privacy settings for the changing context [27].

However, our work, by unpacking the change of context when bystanders are streamed, reports the difficulties to address the change of context if streamers and bystanders manage privacy independently, which points to the need of privacy design to support the collaborations between streamers and bystanders. From the streamers' perspective, when bystanders are not involved in live streaming, the information subjects are the streamers. Streamers disclose their own personal information in the streams. However, when bystanders are streamed, the data subject changes

from the streamer only to both bystanders and the streamer. Streamers disclose not only their own information, but also the bystanders' information. Thus, the context changes, so does the appropriateness of information flow.

While it might be easy to notice the change of data subject in other settings (i.e., collaborative photo-sharing), it is not easy for streamers to realize the change of data subject on their own during live streaming because: 1) most bystanders in our study live with streamers, such as parents, roommates, and siblings. Streamers are accustomed to having these bystanders sitting next to them, talking to them and walking around them in everyday life. They might interact with their bystanders without realizing the change of the data subject and the change from real life to live streaming, which violates bystanders' privacy. For example, P23 mentioned that she accidentally chatted with a teammate about him (the friend) being broke up on Valentine's Day through voice chat in streaming regardless the context had changed which made the friend feel embarrassed. 2) most bystanders appear in the streaming out of sudden. Streamers have little time to withhold bystanders' information due to the real-time nature of live streaming, even when they do want to protect bystanders' privacy. This leads to the unexpected leakage of bystanders' information. For example, P10 mentioned that even if he tried to avoid his parents being streamed by scheduling streaming when his parents were not at home, his parents sometimes suddenly came back and were unexpectedly streamed. 3) most streamers had to handle multiple tasks during live streaming. They need to create interesting performance to attract and interact with audience [39, 40, 57, 77, 80]. Trying to notice the change of data subject will increase their cognitive workload, making it difficult to address the change of context in live streaming. As such, it puts too much labor on the streamers to deal with the change of the context alone. If bystanders could alert streamers before they come close to the live streaming, streamers can better protect their privacy.

In addition, while we did not interview bystanders directly, one important insight from our study is that bystanders also need to realize the change of context and cooperate with the streamers, as several steamers we interviewed emphasized how they wished their bystanders to be more aware of the live streaming in progress. To bystanders, the change of context is that the senders of their information is no longer bystanders themselves, but also include the streamers. The change of data sender requires bystanders to make appropriate changes to their information disclosure.

In our findings, bystanders failed to realize the change in context on their own, which confirms prior work's findings. Prior work has shown that due to the invisibility of the streaming devices, bystanders often have no idea whether the streaming is ongoing [21]. For instance, bystanders in Faklaris et al.'s study expressed that they had a difficult time figuring out if the streamer was streaming or simply playing game or talking to someone when they saw someone was using their phones in public places [21]. Our work is inline with this prior work by showing that it is challenging for bystanders alone to realize the change of context.

What we move beyond prior work is that we find additional challenges for bystanders to handle the changing context that require the coordination between both streamers and bystanders. In our study, one big challenge for bystanders when the context changes is that they do not know how to moderate the way they talk and behave to protect their privacy in live streaming even though they know live streaming and are able to realize the change of context. These bystanders do not fully understand who would get access to their information and what consequences they would have after disclosing, which requires streamers' input to help them. For example, P5's 9-year-old brother would intrude her streaming and interact with her audience without knowing the negative consequences brought by his participation. P24 hoped her roommates to be more aware when they said each other's real names and disclosed their apparels during streaming. However, there is no existing mechanism that allows streamers and bystanders to work together on the change of context.

Therefore, both streamers and bystanders need to be aware of the change of context and manage their disclosure based on the contextual appropriateness. When data sender and subject are not about the same individual, Contextual Integrity is a collective effort between both stakeholders. Both streamers and bystanders should understand and agree on what should be shared and whom should be shared with to better protect bystanders' privacy. Technical interventions that facilitate the awareness of the change of context in live streaming should also be convenient, which we will discuss in the next section.

8.3 Design Implications

Our findings point to a number of practical design considerations for the future live streaming platform to secure bystanders' privacy. To support shared decision-making between streams and bystanders (Section 6.1), live streaming platforms should provide more channels for bystanders and streamers to communicate each other's privacy preferences and possible privacy consequences. One approach to address this is to bridge streamers' and bystanders' understandings through online tutorials about possible privacy consequences. For instance, the live streaming platforms can ask streamers to complete an online tutorial before first-time streaming about privacy consequences of disclosing sensitive personal information, including those that can happen to bystanders. The platform can provide extra incentives if the streamers invite their bystanders to the tutorials. Another idea is to embed an online discussion session on live streaming platforms in which all the users can share about their experience of being streamed by others. In this way, streamers and bystanders can broaden their understandings about privacy management in live streaming.

To avoid streamers sacrificing bystanders' privacy for enriching streaming content, live streaming tools can provide ways for streamers to block bystanders' identities so that streamers' streaming content will not be influenced. Blocking bystanders' sensitive information in photo/video sharing is not new. Recent attempts have been made to offer different types of obfuscation techniques to block bystanders in collaborative photo-sharing and video sharing, including blurring [44, 61, 73], pixelating [31, 34, 58], masking [3, 25], silhouette (a solid shape of a single colour)[20], inpainting (cutting out undesired parts of an image) [69, 72] and avatar (using avatar to replace the real person) [44, 74]. However, these attempts focus on images. Bystanders' voice, casual chat and inappropriate language can still be unexpectedly exposed. Therefore, intelligent techniques of blocking bystanders' voice should be integrated into live streaming tools. For example, machine learning might be employed to separate bystanders' voice from streamers' voice based on the distance to the speaker and the tones. Separated voice of the bystanders could be transformed through voice-changing techniques. Sensitive information and inappropriate language can be replaced or removed. In addition, inspired by P21's technical strategies of upgrading streaming equipment, the embedded audio system of live streaming can be enhanced to mainly pick up streamers' voice and reduce background sounds so that bystanders' casual chat would not be easily captured during streaming. In this way, bystanders' privacy is preserved, streamers' cognitive burdens will not increase and streaming content will not be badly influenced.

Notification of change of context should be provided to assist streamers and bystanders to be aware of the changing contextual information norms (section 6.2). First, although many live streaming tools have already offered notifications for streamers to notice the change of context, most are about the change of recipients, namely new audience members' joining in. Few of them focus on the change of data subjects when bystanders are streamed. In our interviews, several participants, P5, P7 and P10 mentioned that their bystanders appeared in the streaming out of their expectations, which cannot be addressed through preventative strategies, such as muting microphone and webcam. We thus suggest proximity sensor could be implemented as an app on bystander's smartphone or as an wearable device attached to bystanders' body so as to alert

streamers about the incoming bystanders in advance. When bystanders are about to enter the capture area, streamers could be informed of the incoming bystanders before bystanders are actually captured. Thus, streamers could have more time to prepare their strategies to protect bystanders. Additionally, the sensor can also offer bystanders, especially for those who are reluctant to explicitly express their privacy concerns, a way to communicate their privacy preferences with streamers. They can customize the setting of the sensor based on their privacy need, such as adjusting the range of the alerting area and amplifying the volume of the alert sound. In this way, shared decision-making and communication between streamers and bystanders can be better support in real time.

9 LIMITATIONS AND FUTURE WORK

This research has several limitations that can be addressed in future work. First, we only interviewed streamers in China. Therefore, our results may not be generalizable to streamers in other countries. Prior research has highlighted the cross-cultural differences in users' privacy attitudes and behaviors on social media [41]. Given that all our participants are Chinese, their understanding of others' privacy and strategies adopted to manage others' privacy might be influenced by the Chinese culture. However, it is important to understand bystanders' privacy in a non-western context, which is understudied in prior work. We suggest future work be conducted in other countries and investigate the role of cultural factors in streamers' perception of bystanders' information disclosure.

Second, impacted by the COVID-19 global pandemic, the majority of our participants (24 out of 25) streamed at home. Therefore, most bystanders reported by our participants lived with the participants, such as family, friend and roommate. Only one participant mentioned bystanders who were strangers in outdoor spaces. However, privacy is contextualized based on the relationship between the different stakeholders. It is possible that streamers might have different privacy considerations towards the unknown bystanders or might not care about the unknown bystanders' privacy as much as the bystanders they have close ties with. We suggest future work recruit streamers with more outdoor streaming experience to examine how they evaluate their bystanders' privacy.

Third, although we took streamers' streaming experiences into account when recruiting participants, we only recruited a small portion of full-time streamers (4 out of 25) and popular streamers who had more than 10,000 numbers of viewers (4 out of 25). This is due to the fact that most full-time and popular streamers are bound by contracts with DouYu or other agencies, which prevent streamers from being interviewed. These streamers may have different privacy considerations of their bystanders and employ different strategies to handle bystanders' information disclosure. As a result, we suggest that future study develop better tactics to recruit such streamers. Future work can also consider conducting large-scale quantitative research to investigate if streamers' experiences would significantly affect the way they think of bystanders' privacy.

Fourth, although we recruited our participants through multiple platforms to ensure diversity in the sample, majority of our interviewees were students in college while we also interviewed streamers with different occupations, such as teachers, computer scientist, civil servant and freelancer. This might be due to the fact that most streamers on DouYu are under 24 years old [1] and also streamer is one of the most wanted professions for young students in college [68]. Streamers with different professions or in different age groups may have different perceptions and practices related to managing bystanders' privacy. Therefore, our sample might not well reflect streamers with other occupations or in other age groups.

10 CONCLUSION

In this paper, we interviewed 25 streamers to understand their considerations and practices regarding bystanders' privacy in live streaming. The results suggested that streamers cared about their bystanders' privacy and understood bystanders' privacy based on perceived information sensitivity, perceived bystander's personality and perceived reactions from bystander. To protect bystanders from privacy violations, streamers primarily relied on technical, behavioral and collaborative strategies. Some of these strategies might become ineffective when streamers have to trade bystanders' privacy for attractiveness and when streamers and bystanders share distinct privacy understandings. Thus, more design efforts are needed in future to help streamers protect their bystanders' privacy.

11 APPENDIX A

Interview Questions

Streaming Experience:

What's your gender?

What's your age?

What's your occupation?

Which platform do use for streaming?

Why do you choose this platform(s)?

How long have you been streaming?

Why did you stream?

Streaming Environment:

Where do you stream?

Was there anyone nearby during your broadcasting?

Who were they?

Did they know you were broadcasting?

What were their attitudes towards your live streaming?

What were they doing when you were streaming?

Would you remind them of your streaming? Why?

Did they affect your streaming?

Has anyone ever been streamed in your streaming?

Could you please describe the situation in more detail?

How was the person streamed?

What was the relationship between you and the person?

Was the person aware of being streamed?

What was the person's reaction at that time?

What was your reaction at that time?

Did you take any action at that time?

How did the audience react? Any comments from the audience?

What information of the person was streamed?

Was this information appropriate or inappropriate to be shared with your audience?

Would this information disclosure affect the person? How? Any consequences?

Do you think such information disclosure would affect your streaming?

Has this person ever complained about being streamed to you?

Did you communicate with the person about him being streamed later?

Would such information disclosure affect the relationship between you and him?

What strategies did you use to prevent others' information from being streamed in your

live streaming?

      Could you explain the strategies in more detail?

      When would you use such strategies?

      What do you think of these strategies?

   What features did you often use to prevent others from being streamed?

      What do you think of the features?

      How did you know the settings?

      How did you set up the settings?

      How did you like the settings? Any problems using them?

      What improvement do you suggest for the settings? Why? How?

Besides what you have told us, do you have any other thing you want to share with us regarding other people's information sharing during live streaming?

Have you ever heard of any streamers who accidentally shared others' personal information in live streaming? If yes, what happened? Any consequences? Any insights after hearing such news?

Have you ever heard of any people who were accidentally being streamed their personal information in live streaming? If yes, what happened? Any consequences? Any insights after hearing such news?

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations and Strategies for Bystanders' Privacy Management

127:25

12 APPENDIX B

Theme	Sub-theme	Sub-sub-theme	Codes
Considerations	Based on Perceived Information Sensitivity	Information that streamer perceives sensitive	• Disclosing bystanders' family members and family matters is not ok. • Disclosing bystander's outfit and inappropriate dressing is not ok. • Disclosing bystanders' unsatisfying looks is not ok. • Disclosing bystanders' personal information (eg., job, real name, address) is not ok. • Disclosing bystanders' financial information is not ok. • Disclosing bystanders' social relationships is not ok.
		Information that streamer perceives not sensitive	• It's ok to stream my bystanders' voices. • Bystanders' casual talks are fine to be streamed. • It's appropriate to broadcast bystanders' pseudonyms and nicknames. • It isn't a big deal to disclose bystanders' daily life to my audience.
	Based on Perceived Bystander's Personality		• It's ok to disclose extroverted bystanders' information. • It's not ok to get introverted bystanders involved in the streaming. • I don't stream my bystanders since they don't like being photographed in real life.
	Based on Perceived Reaction from Bystanders	Bystanders mind being streamed	• My bystanders often asked me if I was streaming. • My bystanders often checked the status of my microphone and webcam before/during my streaming. • My bystander would dodge the camera when I was streaming. • My bystander displayed an embarrassing facial expression when he knew he was streamed. • My bystander minimized their exposure when I was streaming. • My bystander changed the subject immediately.
		Bystanders do not mind being streamed	• My bystander acted the same as usual during my streaming. • My bystanders talked or behaved as the way they would do when the live streaming was off.
Strategies	Streamers' Individual Strategies	Technical strategies	• I used the mute button to avoid exposing bystanders' conversations. • I disabled the video feed to protect my bystanders. • I turned off the headset to block my bystander's voice. • I turned off the webcam to protect my bystanders' physical appearance. • I adjusted the angle of the webcam when I found my bystanders were streamed. • I upgraded my streaming equipment to reduce bystanders' voices. • [Challenge] Turning off the webcam/microphone might negatively affect streamers' performance.
		Nontechnical behavioral strategies	• I stream when bystanders are not around. • I used the wall as background. • I locked the door when I was streaming. • I wouldn't order deliveries to avoid the deliveryman being streamed. • [Challenge] It was in conflict with streamers' desired streaming quality.
	Streamer and Bystander's Collaborative Strategies	Led by streamer	• I'll tell my bystanders that I'm going to broadcast. • I'll tell my bystanders if I'm going to use the microphone and/or webcam. • I warned my bystanders every time when they were about to show up. • I asked my bystander not to mention any of his personal information in my streaming.
		Led by bystander	• My bystanders would lower their voices. • My bystander used lip-synching to talk with me. • My bystanders pat my shoulder when they want to talk with me. • My bystanders would gently knock on the wall or desk to let me know that they need to talk with me.
		Mutual norms	• My bystander and I used eye contact and a third-party app to communicate with each other. • My bystanders know what to say and not to say. • My bystanders and I called each others' nicknames. • My brother and I spoke with each other using dialect.

Table 2. Themes, sub-themes and codes

REFERENCES

[1] 20 Million Live Streamers Data (Translated Title). 2019. https://www.pingwest.com/a/193302.

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

[3] Rawan Alharbi, Mariam Tolba, Lucia C Petito, Josiah Hester, and Nabil Alshurafa. 2019. 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 (2019), 1–29.

[4] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[5] Yang ang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. *Proc. Priv. Enhancing Technol.* 2016, 3 (2016), 172–190.

[6] Gaurav Bansal, Fatemeh Mariam Zahedi, and David Gefen. 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management* 53, 1 (2016), 1–21.

[7] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. {Bystanders'} Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*.

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

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

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

[11] Bystander threatens to break Twitch streamer's camera. 2019. https://www.dexerto.com/entertainment/bystander-threatens-to-break-twitch-streamers-camera-1298355.

[12] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 981–992. https://doi.org/10.1145/2858036.2858498

[13] Twitter Help Center. 2022. Private information and media policy. https://help.twitter.com/en/rules-and-policies/personal-information.

[14] Hichang Cho and Anna Filippova. 2016. 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*. 503–514.

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

[16] Ray Crozier and Lynn E Alden. 2009. *Coping with Shyness and Social Phobias: A Guide to Understanding and Overcoming Social Anxiety*. Simon and Schuster.

[17] Prerit Datta, Akbar Siami Namin, and Moitrayee Chatterjee. 2018. A survey of privacy concerns in wearable devices. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 4549–4553.

[18] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. 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*. 2377–2386.

[19] Mariella Dimiccoli, Juan Marín, and Edison Thomaz. 2018. 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 (2018), 1–18.

[20] Alex Edgcomb and Frank Vahid. 2012. Privacy perception and fall detection accuracy for in-home video assistive monitoring with privacy enhancements. *ACM SIGHIT Record* 2, 2 (2012), 6–15.

[21] Cori Faklaris, Francesco Cafaro, Asa Blevins, Matthew A O'Haver, and Neha Singhal. 2020. A snapshot of bystander attitudes about mobile live-streaming video in public settings. In *Informatics*, Vol. 7. Multidisciplinary Digital Publishing Institute, 10.

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

[23] Lewis R Goldberg. 1993. The structure of phenotypic personality traits. *American psychologist* 48, 1 (1993), 26.

[24] Rakibul Hasan, Bennett I Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your Photo is so Funny that I don't Mind Violating Your Privacy by Sharing it: Effects of Individual Humor Styles on Online Photo-sharing Behaviors. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[25] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer experience of obscuring scene elements in photos to enhance privacy. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[26] Rakibul Hasan, Patrick Shaffer, David Crandall, Eman T Apu Kapadia, et al. 2017. Cartooning for enhanced privacy in lifelogging and streaming videos. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*. 29–38.

[27] Yangyang He, Paritosh Bahirat, Bart P Knijnenburg, and Abhilash Menon. 2019. A data-driven approach to designing for privacy in household iot. *ACM Transactions on Interactive Intelligent Systems (TiiS)* 10, 1 (2019), 1–47.

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

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

[30] Iris A Junglas, Norman A Johnson, and Christiane Spitzmüller. 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* 17, 4 (2008), 387–402.

[31] Mohamed Khamis, Habiba Farzand, Marija Mumm, and Karola Marky. 2022. DeepFakes for Privacy: Investigating the Effectiveness of State-of-the-Art Privacy-Enhancing Face Obfuscation Methods. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*. 1–5.

[32] Bart P Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano. 2022. Modern Socio-Technical Perspectives on Privacy.

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

[34] Pavel Korshunov, Andrea Melle, Jean-Luc Dugelay, and Touradj Ebrahimi. 2013. Framework for objective evaluation of privacy filters. In *Applications of Digital Image Processing XXXVI*, Vol. 8856. SPIE, 265–276.

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

[36] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. 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*. 3217–3226.

[37] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[38] Asko Lehmuskallio. 2007. "A photo is not an extension of me, it's plain surface."–Views of users of a Web 2.0 photo-sharing site on photos and privacy. *SPIEL* 26, 2 (2007), 271–289.

[39] Jie Li, Xinning Gui, Yubo Kou, and Yukun Li. 2019. Live streaming as co-performance: Dynamics between center and periphery in theatrical engagement. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–22.

[40] Lingyuan Li, Jirassaya Uttarapong, Guo Freeman, and Donghee Yvette Wohn. 2020. Spontaneous, Yet Studious: Esports Commentators' Live Performance and Self-Presentation Practices. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–25.

[41] Yao Li. 2022. Cross-Cultural Privacy Differences. In *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham, 267–292.

[42] Yao Li and Xinning Gui. 2022. Examining Co-Owners' Privacy Consideration in Collaborative Photo Sharing. *Computer Supported Cooperative Work (CSCW)* (2022), 1–31.

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

[44] Yifang Li, Nishant Vishwamitra, Hongxin Hu, Bart P Knijnenburg, and Kelly Caine. 2017. Effectiveness and users' experience of face blurring as a privacy protection for sharing photos via online social networks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE Publications Sage CA: Los Angeles, CA, 803–807.

[45] Heather Richter Lipford, Andrew Besmer, and Jason Watson. 2008. Understanding privacy settings in facebook with an audience view. *UPSEC* 8 (2008), 1–8.

[46] Zhicong Lu. 2021. *Understanding and Supporting Live Streaming in Non-Gaming Contexts*. Ph. D. Dissertation. University of Toronto (Canada).

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

[48] Zhicong Lu, Haijun Xia, Seongkook Heo, and Daniel Wigdor. 2018. 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*. 1–13.

[49] Ameera Mansour and Helena Francke. 2021. 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 (2021), 1–27.

[50] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "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*. 1–11.

[51] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: An empirical test using context to expose confounding variables. *Colum. Sci. & Tech. L. Rev.* 18 (2016), 176.

[52] Austin Miller Matthew Woods. 2022. Video Game Content Creators Face COPPA Liability Hazards. https://news.bloomberglaw.com/privacy-and-data-security/video-game-content-creators-face-coppa-liability-hazards.

[53] Mike Tomlin Comments on Antonio Brown Posting Video on Facebook Live. 2017. https://bleacherreport.com/articles/2687541-mike-tomlin-comments-on-antonio-brown-posting-video-on-facebook-live.

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

[55] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[56] Helen Nissenbaum. 2009. Privacy in context. In *Privacy in Context.* Stanford University Press.

[57] Jamie oodcock and Mark R Johnson. 2019. The affective labor and performance of live streaming on Twitch. tv. *Television & New Media* 20, 8 (2019), 813–823.

[58] Tribhuvanesh Orekondy, Mario Fritz, and Bernt Schiele. 2018. Connecting pixels to privacy and utility: Automatic redaction of private information in images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 8466–8475.

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

[60] Blaine A Price, Avelie Stuart, Gul Calikli, Ciaran Mccormick, Vikram Mehta, Luke Hutton, Arosha K Bandara, Mark Levine, and Bashar Nuseibeh. 2017. 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 (2017), 1–18.

[61] Moo-Ryong Ra, Seungjoon Lee, Emiliano Miluzzo, and Eric Zavesky. 2017. Do not capture: Automated obscurity for pervasive imaging. *IEEE Internet Computing* 21, 3 (2017), 82–87.

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

[63] Say No to be streamed! It is everyone's legitimate right to refuse to be "live broadcast"(translated title). 2022. http://opinion.voc.com.cn/article/202209/202209050815497632.html.

[64] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. 2016. 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*. 3197–3203.

[65] Thomas Smith, Marianna Obrist, and Peter Wright. 2013. Live-streaming changes the (video) game. In *Proceedings of the 11th european conference on Interactive TV and video*. 131–138.

[66] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*. 521–530.

[67] Anselm L Strauss. 1987. *Qualitative analysis for social scientists.* Cambridge university press.

[68] Streamer is the Most Wanted Profession for Young Students in College (Translated Title). 2018. https://www.sohu.com/a/257458796_695084.

[69] Qianru Sun, Liqian Ma, Seong Joon Oh, Luc Van Gool, Bernt Schiele, and Mario Fritz. 2018. Natural and effective obfuscation by head inpainting. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 5050–5059.

[70] John C Tang, Gina Venolia, and Kori M Inkpen. 2016. 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*. 4770–4780.

[71] Lai Lin Thomala. 2022. Number of live streamers in China 2016-2021. https://www.statista.com/statistics/1061708/china-online-streaming-user-number.

[72] Evgeniy Upenik, Pinar Akyazi, Mehmet Tuzmen, and Touradj Ebrahimi. 2019. Inpainting in omnidirectional images for privacy protection. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2487–2491.

[73] Nishant Vishwamitra, Bart Knijnenburg, Hongxin Hu, Yifang P Kelly Caine, et al. 2017. Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 39–47.

Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations
and Strategies for Bystanders' Privacy Management
127:29

[74] Cheng Yao Wang, Sandhya Sriram, and Andrea Stevenson Won. 2021. Shared Realities: Avatar Identification and Privacy Concerns in Reconstructed Experiences. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–25.

[75] Jason Wise. 2022. TWITCH STATISTICS 2022: HOW MANY PEOPLE USE TWITCH? https://earthweb.com/twitch-statistics..

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

[77] Li Yao Gui Xinning Wisniewski Pamela Wu, Yanlai. 2021. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–26.

[78] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. 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)*. Association for Computing Machinery, New York, NY, USA, 6789–6793. https://doi.org/10.1145/3025453.3026049

[79] Josh Ye. 2019. How Douyu won the live-streaming war to become China's Twitch. https://www.scmp.com/abacus/who-what/what/article/3028270/how-douyu-won-live-streaming-war-become-chinas-twitch.

[80] Ge Zhang and Larissa Hjorth. 2019. Live-streaming, games and politics of gender performance: The case of Nüzhubo in China. *Convergence* 25, 5-6 (2019), 807–825.

[81] Gong Zhe. 2017. Chinese live-streaming platform brought down by privacy concerns. https://www.reuters.com/article/us-china-livestreaming/china-surveillance-streaming-platform-shut-down-amid-privacy-concerns-idUSKBN1EE1OU.

[82] Zhenhui Zhu, Zhi Yang, and Yafei Dai. 2017. Understanding the gift-sending interaction on live-streaming video websites. In *International Conference on social computing and social media*. Springer, 274–285.