Zoombombing: Understanding We-Intention to Engage in Collective Trolling among Online Community Members through the Social Identity Model of Deindividuation Effects

Grace Yuekun Gao
Hong Kong Baptist University
gykgao@life.hkbu.edu.hk

Christy M. K. Cheung
Hong Kong Baptist University
ccheung@hkbu.edu.hk

Tommy K. H. Chan
The University of Manchester
tommy.chan@manchester.ac.uk

Zach W. Y. Lee
The University of Leicester
zach.lee@leicester.ac.uk

Abstract

Zoombombing, the disruptive intrusion into video-conference events, has emerged as a destructive consequence resulting from the wide adoption of collaborative technologies. Despite growing attention from various disciplines, Zoombombing remains underexplored in the field of Information Systems (IS). Recognizing Zoombombing as a form of collective trolling, we aim to uncover the group-referent intention (i.e., we-intention) behind online community members' participation in Zoombombing. Drawing on the social identity model of deindividuation effects (SIDE), we examined how the two aspects of IT-enabled anonymity (i.e., intragroup and intergroup anonymity) exert influence on social elements (i.e., social identities and online disinhibition), ultimately affecting the we-intention to engage collectively in Zoombombing. We validated our research model with a scenario-based survey involving 344 Reddit users. The study contributes to the understanding of Zoombombing as a new form of online collective trolling behavior from the group-referent and sociotechnical perspective and provides insights for research and practice.

Keywords: Zoombombing, Online Community, We-intention, Social Identity Model of Deindividuation Effects (SIDE), Scenario-based Survey

1. Introduction

Zoombombing refers to any practice of disrupting video conference meetings by introducing unwanted content, often including graphic or threatening messages and hate speech (Federal Bureau of Investigation, 2020). This online deviant behavior poses significant threats to businesses and individuals, resulting in privacy and security concerns (Ling et al., 2021), and potential reputation crises for the entities involved (Young 2021). The experiences of Zoombombing also lead to severe trauma among victims, resulting in serious health issues and even loss of life (Lorenz & Alba, 2020). In November 2022, a Chinese teacher tragically died after her online classroom was invaded by a group of uninvited users who disrupted the class by playing loud music and using abusive language (Yin, 2022).

The increasing popularity of online communities provides fertile ground for individuals to engage in Zoombombing campaigns (Elmer et al., 2021; Nakamura et al., 2021). Studies have found that Zoombombing is more likely to be orchestrated by mobs instead of a single attacker, and the coordination of Zoombombing activities is notably prevalent on online platforms like Reddit, 4chan, and Discord (Elmer et al., 2021). Typically, Zoombombing occurs when meeting IDs are unrestrictedly shared in online communities – sometimes by the intended participants of the event. According to Ling et al. (2021), an organized Zoombombing process involves four phases: call for attack, coordination, delivery, and harm. Specifically, in the call for attack phase, a group member initiates attacks on Zoom meetings by posting a thread with detailed meeting information on an online community. The thread created by the member then serves as a central place where potential Zoombombers gather and coordinate their attacks. During the delivery phase, Zoombombers join the meeting and disseminate offensive content to interrupt or even halt the official event. The harmful process is facilitated through the strategic exploitation of Zoom's technological capabilities, including features like screen-sharing, annotation, chat box, and virtual backgrounds.

Given the severe threat of Zoombombing[1], the existing literature has recognized this phenomenon as a

[1] In this paper, hereafter "Zoombombing" refers to the organized Zoombombing behavior.

URI: https://hdl.handle.net/10125/107114
978-0-9981331-7-1

new form of online trolling (e.g., Hacker et al., 2020). However, the prevailing discourse predominantly centers around its prevalence and characteristics (Elmer et al., 2021; Lee, 2022; Ling et al., 2021). Limited attention has been directed towards uncovering the underlying motivations behind this behavior. More specifically, a notable gap remains in our understanding of why and how groups of individuals engage in such online deviant behavior facilitated by information technology. Understanding the group dynamics of Zoombombing is imperative, as such collective trolling behavior holds a greater menace and sometimes can be weaponized for racial harassment and the proliferation of hate speech (Nakamura et al., 2021). In addition, delving into enabling IT characteristics is meaningful to enrich the online trolling literature and steer future interventions, given the integration of technologies allows cyber mobs to assemble swiftly and execute aggressively (Friedberg et al., 2020).

In this regard, this study examines the collective intentions (i.e., we-intention; Bagozzi, 2000; 2007) behind Zoombombing from a sociotechnical perspective (Sarker et al., 2019). Accordingly, we propose the two research questions:

RQ1: Why do members of an online community form a collective intention to participate in Zoombombing?

RQ2: How do the technical and social factors facilitate this collective trolling behavior?

2. Theoretical Background

2.1. Zoombombing

Initially observed during the COVID-19 pandemic when numerous institutions transitioned to online activities, Zoombombing has emerged as a new form of online trolling (Elemer et al., 2021; Hacker et al., 2020). While it shares some similarities with traditional online trolling – the deliberate, antisocial, and provocative behavior aimed at upsetting others (Li et al., 2022) – Zoombombing exhibits distinct characteristics that differentiate itself from its online trolling counterpart.

First, Zoombombing is often characterized by well-organized and group-coordinated efforts across multiple platforms (Elmer et al., 2021; Lorenz & Alba, 2020; Ling et al., 2021; Nakamura et al., 2021). For instance, Elmer et al. (2021) discovered that approximately 41.5% of Zoombombing instances showcased a mob-like raid, where numerous users chaotically infiltrated a Zoom event. Furthermore, the authors also found that this deviant behavior unfolds across multiple platforms. Zoombombers gather in online communities, launch attacks on Zoom, and then share the attack videos on platforms like YouTube. Second, Zoombombing extends beyond mere pranks conducted by Internet trolls to involve the dissemination of harmful content and hate speech that disproportionately targets specific groups of people (Nakamura et al., 2021). Nakamura and colleagues (2021) found that Zoombombing exhibits different patterns in relation to races and genders, with Black communities frequently being targeted. Third, the technical elements afforded by video-conferencing platforms distinguish Zoombombing from other forms of online trolling that typically occur on social networking sites. Specifically, Zoombombers exploit collaborative sharing features to disrupt a meeting by sharing unwanted content in multiple types, including text, video, or audio (Friedberg et al., 2020).

Existing Zoombombing research has primarily consisted of exploratory studies focusing on its prevalence and characteristics (Elmer et al., 2021; Lee, 2022; Ling et al., 2021), the response of Zoom (Young 2021), and the reporting behaviors of victim (Lee & Jang, 2023). However, there is a lack of theory-guided empirical studies, explaining Zoombombing as a well-organized collective trolling behavior. To gain insights into the collective intentions behind Zoombombing, we identified it as a distinct form of online collective trolling occurring across various online platforms, characterized by an organized group effort targeting out-group members (or people with opposite views/opinions on certain topics) using trolling tactics and behaviors (Sun & Fichman, 2020).

2.2. Online Communities and We-intention

Online communities consist of geographically distant individuals with shared interests, forming extensive virtual groups where members may not be personally acquainted or easily identifiable (Sproull & Arriaga, 2007). These virtual forms of communities play a crucial role in providing individuals with supportive information through networking and sharing (Li et al., 2022). For example, Reddit, with approximately 57 million daily active users, serves as the hub for discussions and information sharing in communities organized around specific interests (i.e., subreddits). Within these communities, like-minded individuals gather and communicate (Li et al., 2022). Such a cohesive group resembles the notions of in-group ("us") and out-group ("them") specified in the social identity theory (Tajfel et al., 1971). An in-group is a social category that individuals identify themselves with and perceive themselves as members, whereas an out-group represents a social group that individuals are not part of (Tajfel et al., 1971).

We-intention refers to "a commitment of an individual to participate in joint action [that] involves an

implicit or explicit agreement between the participants to engage in that joint action" (Tuomela, 1995, p. 2). Different from I-intention, which emerges from an individual's independent intent, the we-intention hinges upon mutual understanding in which the group works together toward a collective goal (Cheung & Lee, 2010). Moreover, we-intention is rooted in a shared commitment wherein individual members mutually agree to participate, assuming that other in-group members will engage in similar acts (Tuomela, 1995). In this study, recognizing Zoombombing as a collective behavior instead of an individual-based action, we argue that the concept of we-intention is appropriate for better capturing the group dynamics behind this emerging form of online deviant behavior.

2.3. Social Identity Model of Deindividuation Effects (SIDE)

The SIDE model is a general framework for understanding media effects on online group behaviors and their social psychological processes, particularly with regard to essential IT-enabled features (e.g., anonymity) associated with new media (Chan et al., 2022; Spears, 2017; Spears & Postmes, 2015). Grounded in social identity theory (Tajfel & Turner, 1986) and self-categorization theory (Turner et al., 1987), the SIDE model offers insights into how technological features interact with social features and affect the social psychological processes and outcomes (Spears & Postmes, 2015).

The SIDE model highlights two key aspects of IT-enabled anonymity: "anonymity of" and "anonymity to", which generates two central effects of SIDE, namely the cognitive effect and the strategic effect. According to Spears and Postmes (2015), the cognitive dimension of SIDE proposes that anonymity (of/within the in-group) enhances the salience of social identity, which is the self-awareness of group membership and the emotional and evaluative value of the attachment (Tajfel, 1978). The strategic dimension of SIDE contends that anonymity (to the out-group) may reduce social accountability to out-group members, allowing in-group activities that might otherwise be sanctioned or penalized by the out-group (Spears, 2017).

In the context of our research, anonymity aptly captures the dynamic representation of online groups. When group members participate in Zoom events, they have the ability to manipulate technology designs (e.g., virtual backgrounds, usernames, and profiles) to convey diverse cues related to personal and social identity. Informed by the SIDE model, we further conceptualized the two aspects of anonymity as intragroup anonymity (i.e., anonymity of the in-group) and intergroup anonymity (i.e., anonymity to the out-group) to better investigate the group-referent distinctions in the in-group and out-group context, respectively. Adopting a sociotechnical perspective, we aim to examine how anonymity influences the we-intention to participate in Zoombombing through the perceptions of social identity (i.e., the cognitive mechanism of SIDE) and online disinhibition – a state of reduced restraint and increased comfort in online behavior when one is situated with in-group members (i.e., the strategic mechanism of SIDE). Table 1 presents the definitions of the core constructs in this study.

Table 1. Core Constructs and Definitions

Constructs	Definitions Under Current Research Context
Intragroup Anonymity	The extent to which group members see other in-group members as anonymous, nonidentifiable and interchangeable in an online event on Zoom (Spears & Postmes, 2015).
Intergroup Anonymity	The extent to which group members perceive themselves and other in-group members to be anonymous, nonidentifiable and interchangeable by out-group members in an online event on Zoom (Spears & Postmes, 2015).
Perceived Social Identity	The extent to which in-group members are aware of the membership of the group and the attached value and emotional significance of that membership in an online event on Zoom (Chan et al., 2022; Li et al., 2022).
Perceived Online Disinhibition	The extent to which in-group members' paucity of restraint when communicating in an online event on Zoom (Li et al., 2022; Suler, 2004).
We-intention to Participate in Zoombombing	Online community member's commitment to participate in Zoombombing with the subjective perception that other in-group members will also engage in the Zoombombing (Li et al., 2022).

3. Research Model and Hypothesis Development

Figure 1 depicts the research model. Following the SIDE model, we develop a research model explaining online community members' we-intention to engage in Zoombombing.

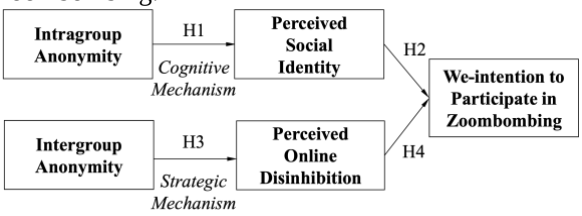

Figure 1. Proposed Research Model

3.1. Cognitive Dimension of SIDE: Intragroup Anonymity and Perceived Social Identity

The cognitive dimension of the SIDE model explains how distinctive IT-enabled features "affect the salience and operation of a particular identity" through depersonalization (Spears & Postmes 2015, p. 33). Depersonalization refers to the tendency to see others as interchangeable group members ("us" in this sense) because individual identities and intra-group differences are obscured under the anonymous condition (Turner et al., 1987). In this regard, individuals in a group-based anonymous online environment may experience a

switch from individual identity to social identity, thereafter forming an enhanced awareness of the crowd by sharing their identity and acting in group norms (Spear & Postmes, 2015; Turner, 1982).

In video-conferencing platforms such as Zoom, users typically have limited access to personal information about others and in-group members often share similar symbols in their names or profile pictures, resulting in difficulties for them to recognize one another. The lack of individuating information makes members see other in-group members as interchangeable, thereby encouraging a more salient social identity and a stronger sense of belonging. This enhanced connection to the group can lead to increased social influence, group awareness, or even group polarization. Furthermore, individuals are more likely to conform to group decisions in social interactions in order to maintain their membership as part of the in-group (Spears & Postmes, 2015). In the context of Zoombombing, we argue that the perception of social identity is a significant factor that influences community members to adhere to the group norm and engage in collective trolling behaviors. Previous empirical evidence has also indicated that the increased social identity within a group further promotes the inclination of members to stereotype out-group members as enemies, thereby facilitating we-intention to engage in collective actions (Cheung & Lee, 2010; Li et al., 2022). Thus, we proposed as follows:

H1. Intragroup anonymity is positively associated with online community members' perception of social identity.

H2. Perceived social identity is positively associated with online community members' we-intention to participate in Zoombombing.

3.2. Strategic Dimension of SIDE: Intergroup Anonymity and Perceived Online Disinhibition

The strategic dimension of the SIDE model explains how IT-enabled features "affect the ability to express identities in line with norms that might be sensitive to surveillance by the audience" (Spears & Postmes 2015, p. 33). Specifically, the structural IT features can offer strategic advantages when computer-mediated communication medium makes individuals less identifiable to out-group, for example, to non-group members and/or powerful authority (Spears, 2017). Previous studies have suggested that one of the major strategic advantages generated by communication technologies is perceived online disinhibition (Li et al., 2022). Online disinhibition is defined as in-group members' paucity of restraint when communicating with others online (Li et al., 2022; Suler, 2004). This perception of online disinhibition has been recognized as one of the key factors resulting in collective deviant behaviors in the online environment (Cheung et al., 2021; Li et al., 2022).

In the context of a Zoom event, participants can control their visibility through Zoom's built-in functions such as turning off their webcams, using a generic username, or utilizing symbols in their profile pictures that are only recognizable to in-group members. In this regard, we argue that when in-group members are afforded anonymity and remain unidentified to out-group members during a Zoom event, they experience diminished inhibitions and restraints. Furthermore, the surroundings by other like-minded members create a psychologically safe state for actively expressing their shared opinions or values, thereby enhancing the collective intention (i.e., we-intention) to participate in Zoombombing. We put forward the following:

H3. Intergroup anonymity is positively associated with online community members' perception of online disinhibition.

H4. Perceived online disinhibition is positively associated with online community members' we-intention to participate in Zoombombing.

4. Research Method

We developed an anonymous online questionnaire and employed the hypothetical scenario method to test our research model. This technique allows respondents to make decisions based on vignettes depicting fictitious characters in hypothetical contexts (Weber, 1992). In the field of IS, the scenario method has been widely used to assess various sensitive and ethical issues, such as security policy violations (Siponen & Vance 2010), computer abuse (D'Arcy et al., 2009), and cyberbullying (Chan et al., 2022). Conducting a scenario-based survey offers several advantages. First, it helps mitigate the challenge of respondents concealing their true intentions and providing socially desirable responses when directly questioned (Trevino, 1992). Second, the scenario method ensures consistent contextual details across respondents, enhancing the analysis and interpretation of their decision-making situations (Alexander & Becker, 1978).

4.1. Scenario Design

We designed the scenario based on real-world news reports from reputable sources, such as the New York Times (e.g., Lorenz & Alba, 2020). The scenario description was further refined after receiving valuable feedback from six social science researchers. In the questionnaire, participants were presented with a textual description and a virtual image depicting a hypothetical Zoombombing scenario. This scenario involved Alex

and several members from their subreddit who infiltrated a Zoom event hosted by a rival group. They engaged in disruptive behaviors, including broadcasting noise and sharing offensive content, ultimately leading to the premature termination of the event.

A pre-test was conducted to further evaluate the scenario design. In the pre-test, we conducted an online survey via Prolific, a data collection service offering reliable, diverse, and high-quality data (Eyal et al., 2022). The target sample consisted of worldwide Zoom users, and we pre-screened participants who have rather high weekly electronic device usage (i.e., at least an hour per day). Participants were asked to evaluate the naturalness of the scenario and rate it in terms of realism, arousal, hurtfulness, and valance on a 7-point Likert scale (1=Strongly disagree to 7=Strongly agree) (Chan et al., 2022). In total, we collected 130 valid responses: 43.1% (n=56) were male, 56.1% (n=73) were female, and 0.8% (n=1) were transgender. The median age of the participants was 26 and most of the participants were aged between 20-26 (56.9%, n=74). Among all participants, 41.5% (n=54) used Zoom for more than one hour a day. The statistical results (Mean (SD) indicate that the hypothetical Zoombombing scenario is perceived as realistic (5.32 (1.028)), highly arousal (6.1 (1.133)), hurtful (6.3 (0.929)) and negative (6.59 (0.712)). Qualitative responses from the open-ended question also demonstrated that most of the participants found the scenario offensive and considered it Zoombombing. Overall, it is suggested that participants had no difficulty recognizing the scenario as "Zoombombing" and felt natural and easy to understand what happened in the scenario.

4.2. Instrument Development

We developed new measurement instruments for our independent variables – the two aspects of anonymity, namely *Intragroup anonymity* (TRA) and *Intergroup anonymity* (TER). Adopting the classic approach proposed by Moore and Benbasat (1991), we carried out a three-phase instrument development process including (1) item creation, (2) scale development, and (3) instrument testing. A considerable number of IS studies (e.g., Cheung et al., 2020) have followed this procedure and added to the repository of rigorous research scales as expected. In the item creation phase, we created an initial pool of 16 items following a two-step procedure (Belk, 2014). First, we collected relevant items from the existing anonymity literature with slight modifications to fit the current context of the in-group and out-group. Second, we generated new items based on the definitions of our focal constructs. In the scale development phase, we conducted card-sorting involving a panel of three experienced social science researchers and three laymen. We removed two items and modified the wording based on the card-sorting results and qualitative feedback toward the items. A total of 14 items measuring TRA and TER were retained. For other focal constructs, we adapted previously validated items to measure them, with slight modifications to fit our current context. Table 2 details the measurements. All the constructs were operationalized as reflective, and the items were measured on a 7-point Likert scale. To detect the social desirability bias and common method bias, we included the Marlowe-Crowne social desirability scale (Reynolds, 1982) and a theoretically unrelated construct "Organizational Commitment" (Herath & Rao, 2009), as the marker variable.

Table 2. Measurements

Constructs	Items	Sample Items	Sources
Intragroup Anonymity	7	Members within my subreddit do not recognize each other during the Zoom event.	Self-developed
Intergroup Anonymity	7	Out-group members do not recognize any members within my subreddit during the Zoom event.	Self-developed
Perceived Social Identity	7	I am a typical member of the subreddit.	Chan et al. (2022)
Perceived Online Disinhibition	4	I feel less nervous engaging in such activities in the Zoom event.	Cheung et al. (2021)
We-intention to Participate in Zoombombing	4	We (i.e., my subreddit members and I) intend to do what they (i.e., Alex and his/her group members) did as described in the scenario.	Li et al. (2022)

To examine the initial reliability of the measuring items and evaluate the flow and clarity of the revised questionnaire, we tested the preliminary version of the full survey instrument within a panel of six social science researchers and considered their comments and feedback in preparing the final version of the questionnaire. We then conducted a pilot test involving 71 Zoom users recruited from Prolific. We calculated Cronbach's alpha (α) and composite reliability (CR) of all the measurement instruments in assessing the reliability of the initial measurements. All items met excellent internal consistency with α and CR values for all constructs were greater than 0.70 (Hair et al., 2019). Therefore, all 31 items remained for the next round of testing. We then conducted exploratory factor analysis (EFA) in SPSS 29.0.0.0 to further assess the validity of the scale. All 31 items were subject to EFA. We applied principal component analysis with EQUIMAX rotation to these items, with 86.04% total variance explained. All items were loaded on the target construct. Based on Hair et al (2019)'s guidance, our acceptable range for factor loading is 0.708. Therefore, we deleted the first two items measuring perceived online disinhibition. We retained all 14 items measuring TRA and TER. As a result, 29 items remained, and the revised questionnaire was also ready for a larger sample of data collection.

4.3. Data Collection and Sample Characteristics

Like the pre-test and pilot test, we recruited our field test samples from Prolific. Our sample included (1) Zoom users and (2) Reddit users who were members of interest communities (i.e., subreddits) where online trolling had been common. Following the pre-screening procedure in Prolific, participants who met our study's criteria were invited to our online questionnaire published via the online survey platform QuestionPro. Reddit is suitable for the current study as its extensive user-created subreddits, commitment to internet anonymity, and large user base. It offers a representative research setting to explore online collective trolling behaviors. Reddit has been selected as the research setting for several Zoombombing exploratory studies and other studies of online collective deviant behaviors (Li et al., 2022). The sample was recruited exclusively from the United States to ensure consistency in the laws and norms regarding social networking platforms (Lowry et al., 2016).

The final version of the questionnaire contained four parts. First, participants were asked to specify one subreddit that they feel most belonged to. We verified the existence of the subreddits by conducting random searches using their exact names. Second, participants were presented with a hypothetical scenario and answered questions related to our main constructs and a marker variable. Third, several open-ended questions were included to collect more background information, such as whether they heard of, witnessed, or participated in a similar scenario and the likelihood of engagement in the future. The final section collected demographic information and included questions about social desirability. To increase data validity, we randomized the order of the questions and included six attention-check questions across sections. Responses were manually reviewed and participants who completed the questionnaire and passed our attention check got 1.5 GBP (around 2 USD). A total of 554 participants attempted the survey, 424 passed the pre-screening questions, and 348 of them completed the entire questionnaire. Four participants were removed from the data set because they (1) failed more than one attention-check question or (2) finished the questionnaire too fast. This resulted in 344 valid responses. Table 3 details the profiles of respondents.

Table 3. Profiles of Respondents

Characteristics	N	%	Characteristics	N	%
Gender			**Members of the focal subreddit**		
Male	196	56.98%	101-500	6	1.74%
Female	133	38.66%	501-1000	12	3.49%
Non-binary	10	2.91%	1001-5000	13	3.78%
Prefer not to say	5	1.45%	5001-10,000	13	3.78%
Age			More than 10,000	300	87.21%
18-24	48	13.95%	**Experience of using the focal subreddit**		
25-34	135	39.24%	Less than 6 months	27	7.85%
35-44	90	26.16%	6-12 months	46	13.37%
45-54	50	14.53%	1-2 years	106	30.81%
55 or older	21	6.10%	3-4 years	90	26.16%
Employment status			5-6 years	46	13.37%
Unemployed	37	10.76%	More than 7 years	29	8.43%
Part-time	50	14.53%	**Daily usage of the focal subreddit**		
Full-time	216	62.79%	Less than 30 minutes	165	47.97%
Student	26	7.56%	30-60 minutes	138	40.12%
Others (retired/disabled)	15	4.36%	1-2 hours	38	11.05%
Education			More than 3 hours	3	0.87%
Less than high school	4	1.16%	**Experience of joining Zoom**		
High school or equivalent	31	9.01%	Less than 6 months	14	4.07%
Some university but no degree	87	25.29%	6-12 months	11	3.20%
Associate's degree	25	7.27%	1-2 years	89	25.87%
Bachelor's degree	145	42.15%	3-4 years	193	56.10%
Master's degree	39	11.34%	5-6 years	25	7.27%
Doctoral degree	13	3.78%	More than 7 years	12	3.49%
Annual income			**Daily usage of Zoom**		
Less than 15,000 USD	69	20.06%	Less than 30 minutes	225	65.41%
15,000 - 35,000 USD	61	17.73%	30-60 minutes	75	21.80%
35,000 - 75,000 USD	124	36.05%	1-2 hours	33	9.59%
75,000 - 150,000 USD	73	21.22%	3-4 hours	7	2.03%
More than 150,000 USD	17	4.94%	More than 5 hours	4	1.16%

5. Data Analysis and Results

We employed partial least squares structural equation modeling (PLS-SEM) to test the research model. The PLS approach is appropriate for this study because it works well in testing a theoretical framework from a prediction perspective and can be used for data that are not normality distributed (Hair et al., 2019). Following Hair et al (2019)'s two-step analytical approach, we tested the measurement model to ensure the reliability and validity of the measures, followed by examining the structural model. The SmartPLS 4 software package was used for the data analysis.

5.1. Measurement Model

We evaluated the reliability, convergent validity, and discriminant validity of the measurement items. To assess the internal consistency of the measurement items, we used Cronbach's alpha (α) and composite reliability (CR). As shown in Table 4, Cronbach's alpha and CR values for all constructs are higher than 0.7, demonstrating good internal consistency (Hair et al. 2019). The convergent validity was tested by (1) assessing the average variance extracted (AVE), which also exceeds the threshold of 0.5 (Hair et al. 2019); and by (2) examining the item loadings on the theoretically assigned constructs, which are all higher than 0.7 (Hair et al., 2019). The results indicated a high degree of convergent validity. To assess the discriminant validity, we applied three criteria: (1) the square root of the AVE for each construct, (2) the heterotrait–monotrait ratio of correlations (HTMT) among constructs, and (3) the cross-loading of measurement items. As shown in Table 5, the square root of the AVE for each construct exceeds its correlation coefficients with others (Hair et al., 2019). The HTMT values for all the constructs, ranging from 0.298 to 0.819, are below the threshold of 0.85, and all items load higher than 0.7 on their corresponding constructs (Hair et al., 2019). The results provided

evidence of a good discriminant validity of our measurement items. We then calculated the variance inflation factor (VIF) to assess multicollinearity. The results revealed that multicollinearity is not a severe issue as the VIF values, ranging from 1.236 to 2.939, are below the threshold of 3.3 (Kock & Lynn, 2012). We also tested common method bias (Podsakoff et al., 2003). First, the Harman's one-factor results indicated the first factor accounted for 45.9% of variance, not exceeding the 50% threshold. Second, correlations between the marker variable and focal constructs were also minimal, ranging from -0.012 to 0.037. Thus, the common method bias had minimal impact on this study.

Table 4. Psychometric Properties of the Measurement Items

Constructs	α	CR	AVE	Items	TRA	TER	POD	PSI	WPZB
Intragroup Anonymity	0.951	0.960	0.773	TRA1	**0.876**	0.677	0.308	0.254	0.419
				TRA2	**0.914**	0.738	0.336	0.261	0.424
				TRA3	**0.867**	0.607	0.306	0.266	0.419
				TRA4	**0.816**	0.662	0.299	0.188	0.357
				TRA5	**0.905**	0.740	0.349	0.295	0.440
				TRA6	**0.902**	0.734	0.344	0.251	0.449
				TRA7	**0.869**	0.706	0.326	0.283	0.411
Intergroup Anonymity	0.979	0.983	0.889	TER1	0.745	**0.948**	0.407	0.357	0.498
				TER2	0.763	**0.953**	0.407	0.362	0.485
				TER3	0.753	**0.927**	0.405	0.338	0.461
				TER4	0.711	**0.929**	0.378	0.362	0.427
				TER5	0.747	**0.952**	0.399	0.372	0.451
				TER6	0.761	**0.955**	0.392	0.342	0.448
				TER7	0.737	**0.936**	0.386	0.373	0.446
Perceived Online Disinhibition	0.906	0.934	0.779	POD1	0.270	0.342	**0.868**	0.277	0.201
				POD2	0.331	0.336	**0.863**	0.355	0.285
				POD3	0.364	0.397	**0.908**	0.306	0.241
				POD4	0.331	0.404	**0.891**	0.315	0.260
Perceived Social Identity	0.952	0.961	0.778	PSI1	0.293	0.392	0.339	**0.928**	0.413
				PSI2	0.284	0.361	0.309	**0.917**	0.400
				PSI3	0.288	0.389	0.270	**0.821**	0.435
				PSI4	0.219	0.294	0.267	**0.898**	0.392
				PSI5	0.228	0.268	0.343	**0.850**	0.399
				PSI6	0.238	0.271	0.344	**0.856**	0.400
				PSI7	0.265	0.350	0.323	**0.900**	0.374
We-intention to participate in Zoombombing	0.974	0.981	0.927	WPZB1	0.454	0.487	0.274	0.418	**0.953**
				WPZB2	0.450	0.467	0.254	0.462	**0.962**
				WPZB3	0.466	0.457	0.276	0.429	**0.970**
				WPZB4	0.464	0.468	0.279	0.450	**0.967**

Note: α=Cronbach's alpha; CR=composite reliability; AVE=average variance extracted; Intragroup Anonymity=TRA; Intergroup Anonymity=TER; Perceived Online Disinhibition=POD; Perceived Social Identity=PSI; We-intention to Participate in Zoombombing=WPZB

Table 5. Correlation Matrix

Constructs	Mean	SD	VIF	TRA	TER	POD	PSI	WPZB
Intragroup Anonymity	3.65	1.691	2.692	**0.879**				
Intergroup Anonymity	3.63	1.827	2.939	0.791	**0.943**			
Perceived Online Disinhibition	4.23	1.638	1.236	0.369	0.420	**0.883**		
Perceived Social Identity	3.80	1.690	1.288	0.296	0.380	0.356	**0.882**	
We-intention to participate in Zoombombing	2.55	1.759	-	0.476	0.488	0.281	0.457	**0.963**

Note: 1. SD=Standard Deviation; VIF=Variance Inflation Factor; Intragroup Anonymity=TRA; Intergroup Anonymity=TER; Perceived Online Disinhibition=POD; Perceived Social Identity=PSI; We-intention to Participate in Zoombombing=WPZB 2. All correlations are significant at the 0.01 level (2-tailed). 3. The diagonal elements in bold represent the square root of AVE.

5.2. Structural Model

A bootstrap with 5000 resamples of the data was performed to test the significance levels of the path coefficients (Hair et al., 2019). Figure 2 shows the data analysis results. As expected, all of the four hypotheses were supported. The results revealed that the intragroup anonymity was positively associated with perceived social identity (β = 0.301, p < 0.001), and the latter was also positively correlated with the we-intention to participate in Zoombombing (β = 0.400, p < 0.001). In terms of the strategic dimension, the results showed that intergroup anonymity was positively associated with perceived online disinhibition (β = 0.423, p < 0.001), which was also positively associated with the we-intention to participate in Zoombombing (β = 0.131, p < 0.05). We also examined the effects of major demographic factors. We found that the size of online community was negatively associated with the we-intention to participate in Zoombombing (β = -0.394, p < 0.05). Other demographic variables including age, gender, and Zoom experience had no statistically significant effect on we-intention to Zoombombing. Overall, the model explains 24.8% of the variance in the we-intention to participate in Zoombombing, with 9.1% of the variance in social identity and 17.7% of the variance in online disinhibition. To measure the model's predictive relevance, we also calculated the Q squares, which were all above zero for the dependent variables.

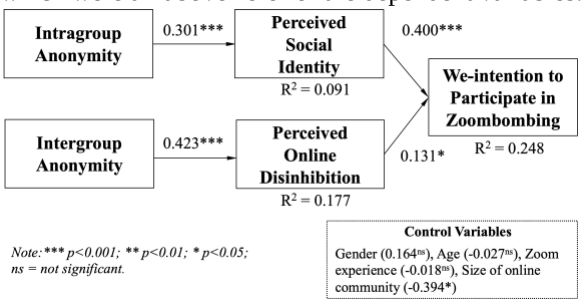

Figure 2. Results of the Research Model

6. Discussion

6.1. Key Findings

Our data analysis results illustrated the relevance of the SIDE model in explaining Zoombombing behavior. Specifically, we examined how the two types of anonymity predict the collective action through two major mechanisms of the SIDE model: cognitive mechanism and strategic mechanism. The intragroup anonymity was positively associated with perceived social identity, which positively affected we-intention to engage in Zoombombing (i.e., the cognitive mechanism). We also found that intergroup anonymity was positively correlated to perceived online disinhibition, which influenced online community members' we-intention to participate in collective trolling behavior (i.e., the strategic mechanism).

To further investigate we-intention to participate in Zoombombing, we explored the roles of major demographic factors. We found that group size had a

significant negative influence on members' participation in Zoombombing. In other words, members in a larger community (i.e., subreddits in our study) are less likely to form we-intention to engage in Zoombombing. One possible reason is that it becomes more difficult to ensure cohesion and consensus among members as the group size increases. This can lead to decreased commitment and coordination, potentially reducing the intention to participate in collective behavior. Some qualitative feedback from respondents provides supportive evidence. For example, one respondent indicated that "…*the subreddit I named is a very large one, I think it would be difficult to get all/many of the members to agree to do something like this.*" Similarly, another respondent wrote: "…*it is a very huge group… even if there was a chance, it would have to be a subgroup of a subgroup to participate*…".

6.2. Theoretical Implications

The current study makes several theoretical contributions. First, our study enriches the understanding of Zoombombing, an emerging deviant behavior resulting from the widespread use of video conference platforms (Elmer et al., 2021; Ling et al., 2021; Nakamura et al., 2021). As one of the first IS studies on this phenomenon, we extend the existing Zoombombing literature by conceptualizing this well-organized adversarial behavior as a novel form of online collective trolling. By approaching Zoombombing from the perspective of group-referent intentional action and drawing on the SIDE model, we emphasized the unique role of Zoom-enabled IT features (i.e., anonymity) and how they interact with social features (i.e., social identities and online disinhibition), providing a rich understanding of the phenomenon from a sociotechnical perspective. By empirically exploring this underexplored online trolling behavior in terms of collective intention, IT facilitation, and harmfulness, our research also broadens the current online trolling literature (e.g., Sun & Fichman, 2020).

Second, our study contributes to the advancement of the SIDE model. By contextualizing the SIDE model in the video-conferencing context, we extend its application beyond the original grounding in text-based computer-mediated communication (Spears & Postmes, 2015). We, therefore, offer insights for future research into applying the SIDE model in diverse communication contexts. Besides, we take a nuanced approach to conceptualize and operationalize anonymity, capturing the distinct online representation within and between groups informed by the SIDE model. Anonymity has long been recognized as a complex construct and has been operationalized in various ways in prior research (Chan et al., 2022; Li et al., 2022; McLeod, 1997; Pinsonneault & Heppel, 1997). However, none of these approaches specifically tackle the crucial group-referent difference that is essential for understanding collective behavior. In line with the rigorous IS paradigm, we have developed a set of 14 items to operationalize both intragroup anonymity and intergroup anonymity, addressing the call to investigate the differential impact of anonymity on collective actions (Li et al., 2022).

Third, our research furthers IS discourses regarding we-intention on underexplored online deviant behavior. Although numerous IS studies have employed the concept of we-intention to examine group-referent intentional behavior in multiple online contexts (Cheung et al., 2011; Cheung & Lee, 2010), there exists a scarcity of research exploring negative online behaviors, with only a handful of exceptions (e.g., Li et al., 2022). The current study informed this stream of "dark side" of technology use research by delving into a new form of online deviant behavior that may cause traumatic consequences.

6.3. Practical Implications

Our research offers practical insights for multiple market players. First, video-conferencing platforms have the potential to adjust their built-in features to manipulate the perceived anonymity in general, which plays a fundamental role in shaping we-intention to participate in Zoombombing. For instance, Zoom could ask for more customizable information to be displayed on users' Zoom profiles (e.g., gender, location, Zoom experience) so that more individuating information can be obtained by users, reducing the formation of salient social identity. Zoom could implement measures such as requesting users to provide additional personal information (e.g., email address, name, phone numbers) when joining a meeting on the basis of protecting their privacy. By doing so, users may feel less disinhibited and more accountable for conducting deviant behavior.

Second, as Zoombombing is a well-organized effort that needs coordination across platforms, online community owners should also take measures to prevent users from taking advantage of the platform's anonymous nature in initiating such attacks (Chan et al., 2022). Strict platform-wide rules should be implemented to restrict content related to Zoombombing and similar activities. Notably, on Reddit, the r/ZoomRaidCodesActive community remains active, with members continuously sharing Zoom codes and organizing Zoombombing incidents.

Lastly, for business sectors or groups vulnerable to Zoombombing, the current study also offers insights for them to prevent such deviant behavior beforehand. For example, they can utilize function configurations that de-anonymized participants, such as restricting meeting

participants to signed-in users only and disabling name and profile changes during meetings.

6.4. Limitations and Future Research Directions

Our study is subject to some limitations. First, while we aimed to create a realistic scenario based on news reports, it is important to note that vignettes may not fully capture the complexity of real-world Zoombombing incidents. Future research could employ scenario-based methods that introduce variations across different conditions to explore the nuances of this phenomenon more comprehensively. Second, our research model was tested using samples from the United States, gathered from a single social platform, Reddit. Future studies can benefit by testing the model in different online communities and cultural backgrounds for more generalized findings. Third, our study primarily focused on testing the SIDE model. Future research could investigate the potential boundary effects of unique technical features in video conferencing platforms, such as webcams and virtual backgrounds. For example, the visibility of other participants and factors such as uniformity in names, virtual backgrounds, or profile photos may influence the perception of social identity and online disinhibition among in-group and out-group members. Finally, while Zoombombing extends across platforms, our research primarily concentrated on its manifestation within video conferencing platform. It would be interesting if future research can delve into this coordinated behavior from a cross-platform perspective. Investigating the dynamics of cross-platform group interactions within online communities and videoconferencing platforms could offer fresh insights into and a more comprehensive understanding of the phenomenon.

7. Conclusion

As one of the first IS studies examining Zoombombing, our research enhances the scientific understanding of Zoombombing as a group-referent and sociotechnical phenomenon. Drawing on the SIDE model, we provided a research model to explain online community members' we-intention to engage in Zoombombing. Our findings indicate the roles of two unique aspects of IT-enabled anonymity in affecting social elements, the latter predicting the we-intention to participate in Zoombombing. These findings also provide practical implications for video-conferencing platforms, online communities, and organizations to prevent the destructive phenomenon.

8. Acknowledgement

This work was supported by a fellowship award from the Research Grants Council of the Hong Kong Special Administrative Region, China [HKBU SRFS2021-2H03].

9. References

Alexander, C. S., & Becker, H. J. (1978). The use of vignettes in survey research. *Public Opinion Quarterly*, *42*(1), 93-104.

Bagozzi, R. P. (2000). On the concept of intentional social action in consumer behavior. *Journal of Consumer Research*, *27*(3), 388-396.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems*, *8*(4), 3.

Belk, R. (2014). You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research*, *67*(8), 1595-1600.

Chan, T. K. H., Cheung, C. M. K., Benbasat, I., Xiao, B., & Lee, Z. W.Y. (2022). Bystanders Join In Cyberbullying on Social Networking Sites: The Deindividuation and Moral Disengagement Perspectives. *Information Systems Research*. Advance online publication.

Cheung, C. M. K, Wong, R. Y. M., & Chan, T. K. H. (2021). Online disinhibition: conceptualization, measurement, and implications for online deviant behavior. *Industrial Management & Data Systems*, *121*(1), 48-64.

Cheung, C. M. K., & Lee, M. K. O. (2010). A theoretical model of intentional social action in online social networks. *Decision Support Systems*, *49*(1), 24-30.

Cheung, C. M. K., Chiu, P. Y., & Lee, M. K. O. (2011). Online social networks: Why do students use Facebook? *Computers in Human Behavior*, *27*(4), 1337-1343.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Elmer, G., Neville, S. J., Burton, A., & Ward-Kimola, S. (2021). Zoombombing during a global pandemic. *Social Media+ Society*, *7*(3).

Eyal, P., David, R., Andrew, G., Zak, E., & Ekaterina, D. (2022). Data quality of platforms and panels for online behavioral research. *Behavior Research Methods*, *54*,1643-1662.

Federal Bureau of Investigation. (2020, April 7). U.S. Attorney Scott Brady and Pennsylvania Attorney General Josh Shapiro warn against Zoom-bombing and hacking teleconferences during coronavirus pandemic. https://bit.ly/3CsAJqS

Friedberg, B., Lim, G., & Donovan, J. (2020). Space invaders: The networked terrain of Zoom bombing. *Technology and Social Change Research Project*.

Hacker, J., vom Brocke, J., Handali, J., Otto, M., & Schneider, J. (2020). Virtually in this together–how web-conferencing systems enabled a new virtual togetherness

during the COVID-19 crisis. *European Journal of Information Systems*, *29*(5), 563-584.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, *13*(7), 546-580.

Lee, C. S. (2022). Analyzing Zoombombing as a new communication tool of cyberhate in the COVID-19 era. *Online Information Review*, *46*(1), 147-163.

Lee, C. S., & Jang, A. (2023). Sharing experiences and seeking informal justice nline: A grounded theory analysis of Zoombombing victimization on Reddit. *Victims & Offenders*, *18*(5), 988-1007.

Li, Y. J., Cheung, C. M. K., Shen, X. L., & Lee, M. K. O. (2022). When socialization goes wrong: Understanding the we-intention to participate in collective trolling in virtual communities. *Journal of the Association for Information Systems*, *23*(3), 678-706.

Ling, C., Balcı, U., Blackburn, J., & Stringhini, G. (2021). A first look at Zoombombing. *2021 IEEE Symposium on Security and Privacy*, *USA*, 1452-1467.

Lorenz, T., & Alba, D. (2020, April 3). "Zoombombing" becomes a dangerous organized effort. *New York Times*. https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html?smid=url-share

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, *27*(4), 962-986.

McLeod, P. (1997). A comprehensive model of anonymity in computer-supported group decision making. *Proceedings of the 18th International Conference on Information Systems (ICIS), USA*, 223-234.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

Nakamura, L., Stiverson, H., & Lindsey, K. (2021). *Racist Zoombombing*. Routledge.

Pinsonneault, A., & Heppel, N. (1997). Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *Journal of Management Information Systems*, *14*(3), 89-108.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.

Reynolds, W. M. (1982). Development of reliable and valid short forms of the Marlowe‐Crowne Social Desirability Scale. *Journal of Clinical Psychology*, *38*(1), 119-125.

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline: Its historical legacy and its continued relevance. *MIS Quarterly*, *43*(3), 695-720.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Spears, R. (2017). Social identity model of deindividuation effects. In P. Rössler, C. A. Hoffner, & L. van Zoonen (Eds.), *The international Encyclopedia of Media Effects* (pp. 1-9). Wiley-Blackwell.

Spears, R., & Postmes, T. (2015). Group identity, social influence, and collective action online. In S.S. Sundar (Ed.), *The Handbook of the Psychology of Communication Technology* (pp. 23-46). Blackwell.

Sproull, L. & Arriaga, M. (2007). Online communities. In Bigdoli, H (Ed.), *The Handbook of Computer Networks* (pp. 248-279). John Wiley & Sons.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, *7*(3), 321-326.

Sun, L. H., & Fichman, P. (2020). The collective trolling lifecycle. *Journal of the Association for Information Science & Technology*, *71*(7), 770-783.

Tajfel, H. (Ed.). (1978). Interindividual behavior and intergroup behavior. *Differentiation between social groups: Studies in the social psychology of intergroup relations* (pp. 27-60). Academic Press.

Tajfel, H. & Turner, J. C. (1986). The social identity theory of intergroup behavior. In Worchel, S., & Austin, W. G (Eds.), *Psychology of Intergroup Relations* (pp. 7-24). Nelson-Hall.

Tajfel, H., Billig, M. G., Bundy, R. P., & Flament, C. (1971). Social categorization and intergroup behavior. *European Journal of Social Psychology*, *1*(2), 149-178.

Trevino, L. K. (1992). The social effects of punishment in organizations: A justice perspective. *Academy of Management Review*, *17*(4), 647-676.

Tuomela, R. (1995). *The importance of us: A philosophical study of basic social notions.* Stanford University Press.

Turner, J. (1982). Toward a cognitive definition of the group. In H. Tajfel (Ed.), *Social Identity and Intergroup Relations*. Cambridge University Press.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). *Rediscovering the social group: A self-categorization theory*. Basil Blackwell.

Weber, J. (1992). Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly*, *2*(2), 137-160.

Yin, C. (2022, November 3). Bullying a concern as teacher dies after online class. *China Daily*. https://www.chinadaily.com.cn/a/202211/03/WS636316fba310fd2b29e80047.html

Young, S. (2021). Zoombombing your toddler: User experience and the communication of Zoom's privacy crisis. *Journal of Business and Technical Communication*, *35*(1), 147-153.