Mind the Gap: Mapping Wearer–Bystander Privacy Tensions and Context-Adaptive Pathways for Camera Glasses

Xueyang Wang
Tsinghua University
Beijing, China
wang-xy22@mails.tsinghua.edu.cn

Kewen Peng
University of Utah
Salt Lake City, Utah, USA
astrid.peng@utah.edu

Xin Yi*
Tsinghua University
Beijing, China
Beijing Academy of Artificial Intelligence
Beijing, China
yixin@tsinghua.edu.cn

Hewu Li
Tsinghua University
Beijing, China
lihewu@cernet.edu.cn

Abstract

Camera glasses create fundamental privacy tensions between wearers seeking recording functionality and bystanders concerned about unauthorized surveillance. We present a systematic multi-stakeholder evaluation of privacy mechanisms through surveys (N=525) and paired interviews (N=20) in China. Study 1 quantifies expectation-willingness gaps: bystanders consistently demand stronger information transparency and protective measures than wearers will provide, with disparities intensifying in sensitive contexts where 65–90% of bystanders would take defensive action. Study 2 evaluates twelve privacy-enhancing technologies, revealing four fundamental trade-offs that undermine current approaches: visibility versus disruption, empowerment versus burden, protection versus agency, and accountability versus exposure. These gaps reflect structural incompatibilities rather than inadequate goodwill, with context emerging as the primary determinant of privacy acceptability. We propose context-adaptive pathways that dynamically adjust protection strategies: minimal-friction visibility in public spaces, structured negotiation in semi-public environments, and automatic protection in sensitive contexts. Our findings contribute a diagnostic framework for evaluating privacy mechanisms and implications for context-aware design in ubiquitous sensing.

CCS Concepts

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

Keywords

Privacy, Bystanders, Camera Glasses, Privacy Awareness, Consent, Multi-Stakeholder

*Corresponding author.

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791848

ACM Reference Format:
Xueyang Wang, Kewen Peng, Xin Yi, and Hewu Li. 2026. Mind the Gap: Mapping Wearer–Bystander Privacy Tensions and Context-Adaptive Pathways for Camera Glasses. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 28 pages. https://doi.org/10.1145/3772318.3791848

1 Introduction

Wearable camera glasses have rapidly transitioned from experimental prototypes to mainstream consumer products. Ray-Ban Meta Smart Glasses have surpassed 2 million units in global sales [126], while technology companies including Xiaomi, Rayneo, and Rokid have launched competing products (Figure 1). These devices offer compelling functionalities including voice assistants, real-time translation, and AR navigation, while embedding high-resolution cameras within fashionable eyewear designs [17].

This integration creates fundamental privacy tensions absent in traditional photography. Unlike smartphones that require conspicuous gestures, camera glasses enable covert recording through voice commands or subtle touches [127]. Current notification mechanisms prove inadequate: Ray-Ban Stories features only a small white LED that becomes imperceptible in bright environments and meaningless to unfamiliar observers [16, 70, 99]. Consequently, bystanders face unprecedented surveillance risks, including unauthorized facial recognition and AI-based inference [63, 88, 89].

Researchers have proposed various Privacy-Enhancing Technologies (PETs) to address these challenges [28, 90, 94]. Wearer-side interventions include automatic bystander detection and blurring [24, 27] and enhanced recording indicators [20, 58]. Bystander-controlled mechanisms enable recording refusal through wearable markers or gestures [55, 96, 113], but impose significant usability burdens in dynamic settings [137]. Prior work has documented that wearers and bystanders hold different privacy expectations [16, 29, 90], and that multi-stakeholder conflicts arise across sensing technologies from smart homes to AR devices [3, 23, 121].

However, a critical gap persists: while existing work establishes that stakeholder conflicts exist, we lack systematic measurement of *how much* expectations diverge across specific privacy dimensions, *which* mechanisms might bridge these differences versus which face irreconcilable conflicts, and *how* context moderates these gaps.

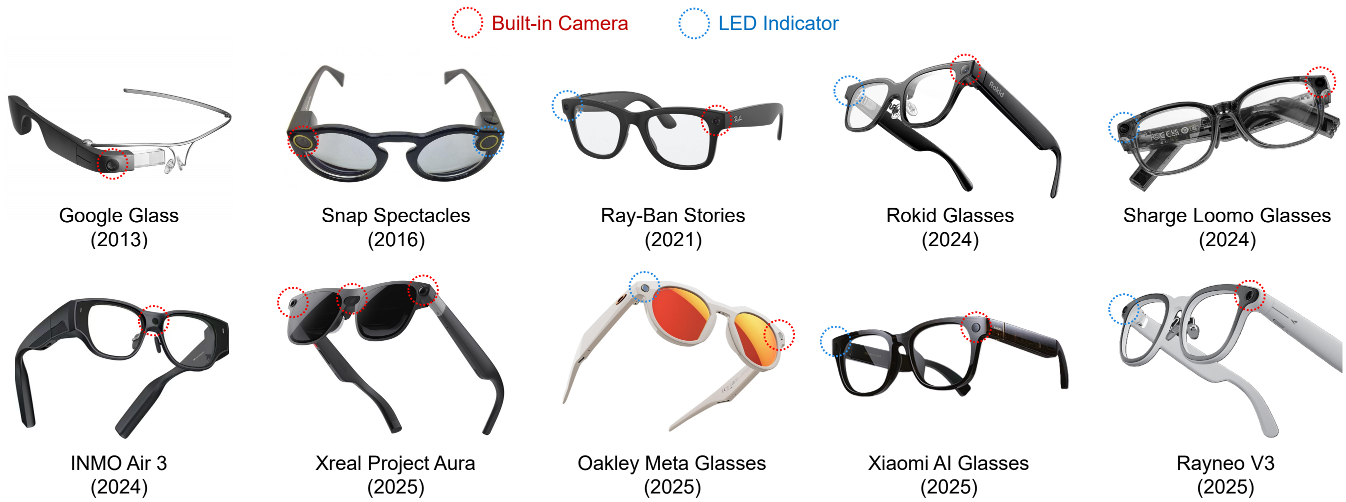

Figure 1: Representative camera-equipped smart glasses launched by major technology companies over the past decade. Their built-in cameras are often seamlessly disguised within everyday eyewear form factors, and LED indicators signaling recording status are typically small, making recording less perceptible to bystanders.

Without such quantification, designers cannot prioritize interventions or anticipate where technical solutions will fail.

To address this gap, we conducted a two-study investigation examining privacy perceptions from both stakeholder perspectives (Figure 2). We situate our study in China, a rapidly growing smart glasses market [135, 136]. While privacy norms vary across cultures, our findings reveal fundamental tensions likely relevant to other contexts [1, 16, 103]. Study 1 employs a large-scale survey (N=525) to quantify privacy expectations across six contextual scenarios varying by physical setting and social relationship. We measured wearers' willingness to provide information transparency and protective measures against bystanders' expectations for these same dimensions. The results reveal persistent expectation-willingness gaps: bystanders demand significantly stronger data sharing control ($p < .01$) and prior consent ($p < .01$) than wearers will provide, with disparities intensifying in sensitive contexts where 65–90% of bystanders would take defensive action.

Study 2 evaluates twelve representative PETs through paired interviews (N=20) combining HCI researchers' theoretical expertise with experienced users' practical insights. Systematic rating across effectiveness, usability, transparency, and social acceptability revealed four fundamental trade-offs: awareness mechanisms that inform bystanders inevitably disrupt social interactions (*visibility versus disruption*), consent mechanisms empower bystanders by burdening them with self-defense (*empowerment versus burden*), automated protection reduces user autonomy (*protection versus agency*), and accountability requires privacy surrender through authentication (*accountability versus exposure*).

These findings point toward a context-adaptive framework that operates through distinct pathways calibrated to environmental characteristics: minimal-friction visibility in public spaces, structured negotiation in semi-public environments, and automatic protection in sensitive contexts where vulnerability justifies reduced autonomy.

Our work makes three contributions to HCI research on ubiquitous sensing privacy:

- **Quantification of expectation-willingness gaps.** Through parallel surveys of 525 wearers and bystanders, we provide systematic measurement of privacy expectation disparities across five information dimensions and five protective measures, revealing that gaps concentrate in control mechanisms and intensify in sensitive contexts.
- **Identification of fundamental trade-offs in PET design.** Through paired evaluation of 12 mechanisms, we identify four trade-offs (visibility versus disruption, empowerment versus burden, protection versus agency, accountability versus exposure) that explain why current approaches fail to reconcile stakeholder conflicts.
- **Context-adaptive privacy pathways.** Based on systematic preference patterns, we propose design pathways that select and combine mechanisms based on environmental characteristics, recognizing context rather than individual negotiation as the primary determinant of privacy acceptability.

2 Related Works

2.1 Privacy Challenges Unique to Camera Glasses

Wearable camera glasses have enabled seamless media capture through integrated cameras and on-device AI, supporting diverse applications from medical assistance [22, 140] to navigation [85] and learning [47]. However, this seamless experience creates distinctive privacy challenges between wearers and bystanders [50, 56, 123].

Unlike web cookies where consent is discrete and individual, camera glasses privacy is situated and dynamic, emerging through ongoing information exchange. Compared with traditional cameras or head-mounted displays (HMDs) like VR/AR headsets, camera

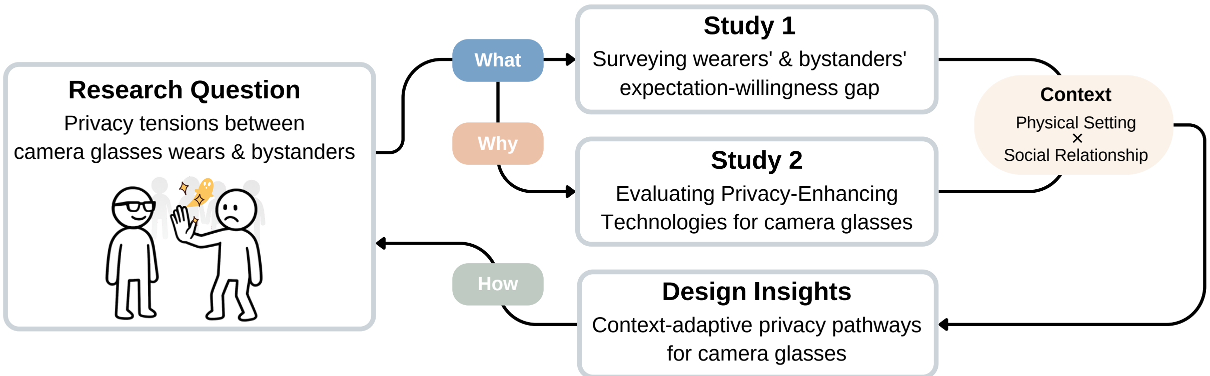

Figure 2: Research framework overview. Study 1 investigates the expectation-willingness gap between wearers and bystanders across contexts (*what* is the gap). Study 2 evaluates existing PETs to understand underlying tensions (*why* the gap persists). Design insights propose context-adaptive pathways (*how* to address the gap).

glasses appear ordinary yet enable continuous recording, intensifying tensions between everyday visibility and pervasive capture. Traditional photography relies on visible gestures (e.g., raising a phone) that signal recording intent [84, 101]. In contrast, camera glasses enable capture through subtle gestures or voice commands [23, 123], leading bystanders to assume continuous recording [56]. Although many devices include LED indicators, such cues often remain imperceptible at distance, easily obstructed, or socially ambiguous [58, 99, 123].

Beyond recording ambiguity, smart glasses transform privacy risks into an instantaneous process through AI-based recognition [50]. Real-time facial recognition and scene understanding provide users with assistance while simultaneously turning bystanders into live data sources before they can become aware or exercise control. This shifts privacy threats from post-hoc content review to real-time inference, where sensitive attributes such as demographics, health status, or affiliations could be extracted [42, 63, 88]. These technical characteristics converge to undermine established social norms for negotiating photography [61]. Traditional phototaking was visually marked and normatively negotiable, enabling bystanders to object or opt out. Smart glasses render such negotiation difficult: wearers may use them as ordinary eyewear without realizing potential offense, while bystanders lack cues to interpret or contest recording [16, 29]. This becomes particularly problematic in sensitive environments such as fitting rooms and medical facilities [83, 107]. These unresolved tensions have repeatedly triggered public backlash and market withdrawals [25, 60].

We summarize these characteristics in Table 1. Collectively, these challenges illustrate that privacy in camera glasses requires re-establishing contextual and social mechanisms for negotiation [69, 125], motivating our examination of context-aware and multi-stakeholder approaches.

2.2 Contextual Factors in Privacy Expectations

Privacy has long been understood as a dynamic boundary-regulation process rather than a fixed state [130]. Altman's theory framed privacy as ongoing negotiation between desired and actual levels of access to the self [11], and subsequent research has consistently shown that privacy expectations shift with where data is captured and who is involved [12, 34, 52]. This pattern is particularly salient in emerging technologies like camera glasses, where users report heightened concern about information being repurposed beyond immediate contexts [40].

Nissenbaum's theory of Contextual Integrity (CI) offers a normative lens for understanding these dynamics [86]. According to CI, privacy violations arise when information flows breach contextual norms of appropriateness (what may be revealed) or distribution (how it may circulate). These norms are shaped by three components: *contextual conditions* that define a setting, the *social roles of actors*, and the *transmission principles* that regulate information flows. For camera glasses, transmission principles for ubiquitous capture remain undefined, making their establishment both urgent and central to our work.

Physical setting has emerged as among the most influential dimensions for understanding camera glasses privacy. Settings structure the visibility and permeability of information flows, influencing whether recording behaviors are perceived as contextually appropriate [12, 86]. Prior research documents that privacy expectations differ significantly across spatial contexts, with tolerance typically higher in public spaces and lower in private or sensitive ones [29, 90]. These expectations reflect situated norms: shared understandings about appropriate behavior within a given space.

Equally critical is the **social relationship** between actors [25, 63, 131]. Prior work in adjacent domains shows that relationship strength (e.g., friend, colleague, stranger) systematically shapes disclosure comfort and privacy expectations [117, 128]. Relationship determines the degree of trust and legitimacy perceived in data capture [5, 39, 91]. With the growing popularity of camera glasses, redefining boundaries between wearers and bystanders has become urgent.

Despite the centrality of context to privacy, prior work has largely examined contextual factors in isolation [5, 29]. O'Hagan et al. [90] systematically varied context in evaluating bystander attitudes toward AR sensing, finding strong effects of both setting and relationship. Windl et al. [132] examined technology-facilitated privacy violations across physical contexts. However, these studies

Table 1: Comparison of privacy-relevant characteristics across recording devices. HMDs refer to head-mounted displays with visible form factors. Camera glasses refer to AI-enabled eyewear resembling ordinary glasses.

Dimension	Privacy Relevance	Camera/Phone	HMD	Camera Glasses
Recording ambiguity	How easily bystanders detect capture intent [84]	High (gestures)	Medium (appearance)	Low (subtle)
Real-time AI processing	Extent of automated recognition at capture [50, 83, 107]	Low (manual)	Medium (task-specific)	High (continuous)
Established social norms	Clarity of shared expectations for recording [16, 29]	High (clear consent)	Medium (emerging)	Low (ambiguous)

primarily capture *single-stakeholder* perspectives. Our work extends this line by systematically comparing how the same contextual factors differentially shape expectations for wearers versus bystanders, revealing where gaps emerge and intensify.

2.3 Stakeholder Perspectives and Privacy Negotiation

Camera glasses create asymmetric privacy relationships where wearers control recording while bystanders bear exposure risks [23]. This asymmetry transforms privacy into continuous negotiation between primary users and secondary actors who often interpret the same recording behavior differently [56].

Bystander-focused research has extensively documented concerns about consent and surveillance. Denning et al. [29] conducted in-situ studies revealing bystanders' discomfort with AR glasses recording. Subsequent work has explored bystander awareness needs [3, 98], defensive responses [115, 141], and protection mechanisms [6, 43, 51]. These studies establish that bystanders consistently desire stronger notification and control than current devices provide.

Wearer-focused research has examined different concerns. Bhardwaj et al. [16] interviewed camera glasses wearers about their privacy dilemmas, finding that many wearers do consider bystander perspectives but face practical constraints in addressing them. Bipat et al. [17] analyzed camera glasses use in the wild, documenting usage patterns and social challenges. Tran et al. [123] surveyed wearers about notification preferences, finding general willingness to signal recording but concerns about social friction.

However, this separation of stakeholder perspectives leaves critical gaps. First, it remains unclear *how much* bystander expectations diverge from wearer willingness across specific privacy dimensions. Second, without direct comparison, we cannot identify which mechanisms might bridge these differences versus which face irreconcilable conflicts. Third, the interaction between stakeholder role and context remains underexplored.

Multi-stakeholder approaches have begun addressing these limitations. Chung et al. [23] examined dyadic interactions through AR glasses, revealing negotiation dynamics but focusing on acquainted pairs. Windl et al. [131] designed consent mechanisms for spontaneous AR interactions, incorporating both user and target perspectives. Abraham et al. [1] explored how sensitive contexts shape both wearer and bystander attitudes toward AR sensing. In smart home contexts, parallel work has examined owner-bystander tensions around domestic cameras [98, 121, 137], demonstrating that multi-stakeholder conflicts are pervasive across ubiquitous sensing technologies.

Our work builds on and extends this foundation in several ways. First, we **quantify** the expectation-willingness gap through large-scale comparative measurement (N=525), enabling precise identification of where stakeholder requirements diverge most sharply. Prior work has documented that gaps exist; we measure their magnitude across specific dimensions and contexts. Second, we systematically evaluate whether existing Privacy-Enhancing Technologies (PETs) can **bridge** these measured gaps, revealing fundamental trade-offs that explain why current approaches fail. Third, we derive empirically-grounded implications for **context-adaptive pathways** that dynamically adjust protection strategies based on the contextual patterns our data reveal. This progression from gap quantification through mechanism evaluation to design recommendations represents a more complete treatment than prior single-study approaches.

2.4 Privacy-Enhancing Technologies for Bystanders

2.4.1 Sensor Transparency and Recording Notification Mechanisms. Recording notifications seek to establish informed consent by enabling bystanders to detect when smart glasses capture audio or video. Current implementations rely primarily on visual indicators—Snap Spectacles employ circular LED rings [58], while Ray-Ban Meta features a "Capture LED" during recording. However, these minimal indicators suffer from fundamental limitations. LEDs assume constant bystander vigilance yet fail when individuals are distracted, facing away, or have sensory impairments [16, 99]. Research confirms that visual indicators alone prove inadequate for conveying device activity awareness [3].

Multimodal notification designs address these limitations by combining visual, auditory, and digital channels. Recent proposals include smartphone notifications to nearby devices and context-sensitive audio alerts [2, 20, 98]. Empirical studies demonstrate user preference for multimodal approaches in privacy-sensitive contexts, though implementation faces inherent tensions between noticeability and obtrusiveness [58, 121]. Smart home research provides relevant precedents through "tangible privacy" mechanisms [3] and privacy visualization systems [8, 100], yet camera glasses' mobility demands solutions optimized for spontaneous encounters rather than controlled environments.

2.4.2 *Empowering Bystander Control and Refusal.*

Beyond awareness, bystanders seek active intervention capabilities to signal recording refusal [75, 95]. One approach employs personal countermeasures: FacePET uses infrared LEDs to blind cameras [96], while InPhysible camouflages physiological signals [79]. Despite experimental effectiveness, these solutions prove impractical by requiring bystanders to carry specialized devices in anticipation of encounters.

Environmental interventions offer broader coverage through infrastructure-based solutions. BlindSpot proposed jamming signals in sensitive spaces [93], while systems like I-Pic and Cardea enable wireless privacy preference broadcasting [2, 112]. These approaches eliminate individual equipment burdens but require industry-wide protocol adoption and regulatory enforcement currently absent from the ecosystem.

Marker-based consent signaling represents a third approach, enabling individuals to wear visual identifiers or perform gestures that trigger automatic recording cessation [19, 55, 113]. However, practical deployment faces critical obstacles: bystanders must anticipate risks and prepare markers, visible indicators may compromise user privacy, and enforcement depends on universal manufacturer compliance. Without mandatory standards, non-compliant devices can simply ignore signals, limiting these solutions to conceptual or prototype stages.

2.4.3 *Automated Bystander Privacy Protection.*

Automated approaches implement privacy protection directly within recording devices through computer vision and signal processing. BystandAR distinguishes interaction targets from bystanders using eye tracking and spatial audio [24], while other systems employ real-time face blurring [9, 43] or activity recognition in degraded images [30]. Contextual factors including location [110], social connections [129], and accessibility needs [134] can drive automatic control decisions. PrivacEye exemplifies sophisticated approaches by using eye movement analysis to detect privacy sensitivity and trigger mechanical shutters [116].

Despite technical advances, automated protection faces fundamental limitations. Bystanders remain unaware of post-processing applications, perpetuating trust deficits regardless of actual protection levels. Recent research highlights risks of overlooking legitimate privacy concerns due to inadequate bystander definitions [87]. Effective deployment requires coordinated ecosystem development including transparency mechanisms, industry standards, and public education, suggesting that technical solutions alone cannot resolve the complex sociotechnical challenges of ubiquitous sensing.

3 Study 1: Surveying Wearers' and Bystanders' Privacy Expectations

To systematically understand privacy expectations surrounding camera glasses, we conducted a large-scale survey examining perspectives from two stakeholder groups: current or potential smart glasses users (*wearers*, N = 232) and individuals potentially affected by such devices (*bystanders*, N = 293). Our scenario-based design evaluated privacy attitudes across situations varying by **physical setting** (public, semi-public, private/sensitive spaces) and **social relationship** (strangers versus acquaintances). This dual-perspective approach enables direct comparison of expectations and identification of conflicts between groups. Study 1 addresses two research questions:

- **RQ1:** How do contextual factors (physical setting and social relationship) influence wearers' and bystanders' privacy concerns and behavioral intentions?
- **RQ2:** What gaps exist between bystanders' expectations and wearers' willingness regarding information transparency and protective measures? How effectively do current notification mechanisms meet stakeholder needs?

3.1 Survey Design

3.1.1 *Contextual Scenario Design.*

Grounded in Contextual Integrity theory [86], we designed six vignettes systematically varying across physical setting and social relationship in a 3×2 design, balancing comprehensiveness with participant fatigue [90, 132]:

- **Public spaces:** Street (travel vlog with companions), Mall (shopping among strangers)
- **Semi-public spaces:** Meeting room (documentation with colleagues), Hospital (consultation among strangers)
- **Private/sensitive spaces:** Private party (casual recording with friends), Gym (workout documentation among strangers)

Each vignette portrayed typical camera glasses use from the participant's assigned role (wearer or bystander), with presentation order randomized using Latin square counterbalancing to reduce sequencing bias [35, 62].

3.1.2 *Technology Primer.*

To address varying familiarity levels across participants, all respondents received a standardized technology primer before evaluation. This primer included: (1) representative product images and brand examples (Ray-Ban Meta, Xiaomi AI Glasses), (2) typical use cases and core functions, (3) annotated photographs showing LED indicator placement, and (4) explanation of LED signaling conventions. This ensured all participants possessed sufficient baseline knowledge for informed responses regardless of prior experience.

3.2 Measures

3.2.1 *Demographics and Baseline Attitudes.*

We collected demographic information including gender, age, education, camera glasses familiarity, and brand awareness. To establish baseline privacy attitudes, we employed validated scales adapted for each stakeholder group (see Appendix A for complete items).

For **bystanders**, we adapted the Internet Users' Information Privacy Concerns (IUIPC) scale [73], measuring three dimensions with two items each: *Awareness* (need for disclosure about data collection), *Control* (perceived control over information practices), and *Collection* (concerns about unauthorized recording).

For **wearers**, we developed scales capturing other-regarding privacy attitudes. Drawing on the Privacy Orientation Scale [15], we created two items measuring *Perceived Responsibility* toward bystanders. We then used Protection Motivation Theory (PMT) [72, 111] as a generative lens to design items capturing *Privacy Protection Intention* (willingness to modify behavior when others object) and *Information Sharing Intention* (willingness to inform bystanders).

We chose PMT over value-oriented scales such as VOPP [44] because our goal was to assess context-specific behavioral intentions rather than general privacy values. While PMT was originally developed for self-protective behaviors, its threat/coping appraisal structure extends naturally to other-regarding contexts, an approach established in healthcare informatics research on protecting patient privacy [64, 71].

Given overall survey complexity (six scenarios × multiple dimensions), we made a deliberate measurement trade-off: baseline attitudes used abbreviated 2-item scales for descriptive purposes, while scenario-based measures, which support our core claims, received greater emphasis.

3.2.2 Contextual Measures. For each scenario, we collected role-specific measures. Bystanders evaluated: privacy concerns (PC(B)), behavioral responses (BH(B)), information needs (I(B)), and protective measure expectations (PT(B)). Wearers assessed: recording reasonability (R(W)), concerns about affecting bystanders (PC(W)), information disclosure willingness (I(W)), and protective measure willingness (PT(W)).

Following prior literature on privacy negotiation [23, 29, 40, 46, 90], we operationalized five information dimensions and five protective mechanisms:

- **Information dimensions:** Purpose (intended use), Content (recording details), Sharing (upload/distribution), Retention (storage duration), AI Use (recognition/analysis)
- **Protective measures:** Proactive Notification, Privacy Filter (face blurring), No Sharing (upload prohibition), Auto Delete, Prior Consent

Both used 7-point matrix-style Likert scales, supplemented by open-ended questions.

3.2.3 LED Indicator Evaluation. Participants evaluated existing LED indicators on: adequacy (5-point scale), inadequacy reasons (multiple choice), preferred notification methods (multiple choice), and adoption motivators (multiple choice).

3.2.4 Scale Development and Validation. Our instrument development followed a rigorous multi-stage process [62]. First, two researchers independently collected candidate items from relevant literature [29, 73, 90, 111], then collaboratively merged similar items and removed semantically ambiguous or construct-inconsistent items. Second, two external experts in cybersecurity and privacy reviewed the instrument to refine wording, ensure non-leading phrasing, and verify accessibility for general audiences. Third, we conducted three iterative pilot rounds (N=5 each), asking participants to identify ambiguous statements and checking for ceiling/floor effects. Feedback was incorporated until no ambiguities were reported.

3.3 Participants and Procedure

We recruited participants from mainland China through distinct channels. Bystanders were recruited via university mailing lists using materials broadly describing the study as examining attitudes toward wearable electronics to avoid response bias. Wearers were recruited through smart glasses enthusiast groups, brand communities, and forums. China provided an ideal research context as the world's largest smart glasses market—IDC projects 2.75 million units shipped in 2025 (107% year-over-year growth) [135], with brands like Xiaomi achieving rapid adoption [136].

Participants completed the 8-minute survey for USD $1 compensation after providing informed consent. Quality controls excluded responses with completion times under 3 minutes, Mahalanobis D^2 outlier detection for straightlining, and failed attention checks, yielding 293 valid bystander responses (18.6% exclusion rate) and 232 valid wearer responses (13.4% exclusion rate).

Sample characteristics reflect typical technology adoption patterns (see Table 9 in Appendix). Wearers exhibited early adopter profiles with higher male representation (59.5% vs. 49.2%), greater device experience (23.3% vs. 4.4% current/former users), and increased awareness of international brands (Ray-Ban Meta: 43.5% vs. 27.0%). Both groups showed high familiarity with domestic brands, particularly Xiaomi AI Glasses (>87%). Including participants with varying familiarity levels reflects real-world market conditions where most potential bystanders are non-users; our goal was to evaluate privacy mechanisms rather than device usability. The substantial sample sizes provide robust coverage across the adoption spectrum, though high education levels (>80% bachelor's degree) may limit broader generalizability.

The study protocol was reviewed and approved by the Institutional Review Board (IRB) of Tsinghua University, and we strictly protected participants' data privacy throughout the study.

3.4 Measurement Validity

Our scenario-based scales demonstrated strong internal consistency: Information Needs (bystanders, $\alpha = 0.89$), Protective Measure Expectations (bystanders, $\alpha = 0.89$), Information Disclosure Willingness (wearers, $\alpha = 0.94$), and Protective Measure Willingness (wearers, $\alpha = 0.93$). Baseline attitude scales showed modest reliability typical of 2-item measures ($\alpha = 0.48–0.77$), appropriate for their descriptive purpose.

To assess convergent validity, we examined correlations between baseline measures and scenario-averaged outcomes (see Figure 14 in Appendix). For bystanders, baseline items correlated positively with scenario-based privacy concerns and protection demands (r ≈ .12–.42, most ps < .001). For wearers, baseline responsibility and intention items correlated moderately with scenario-based disclosure willingness and protection adoption (r ≈ .25–.62, ps < .001). These patterns support treating abbreviated baseline scales as valid descriptive measures, though we acknowledge their limitations for primary analyses. Therefore, we treat these short baseline scales as secondary descriptive measures and do not rely on them as primary evidence for our core claims.

Exploratory factor analyses confirmed construct validity for all scenario-based measures. Each construct yielded a dominant first factor explaining 38.9–61.9% of variance, with item loadings ranging from 0.56 to 0.86 and item-total correlations from 0.50 to 0.83, supporting their use as composite measures.

3.5 Statistical Analysis

We employed the Aligned Rank Transform (ART) procedure [133] to accommodate non-normal Likert-scale distributions. Mixed-design ANOVAs examined Group (between-subjects: wearer vs. bystander)

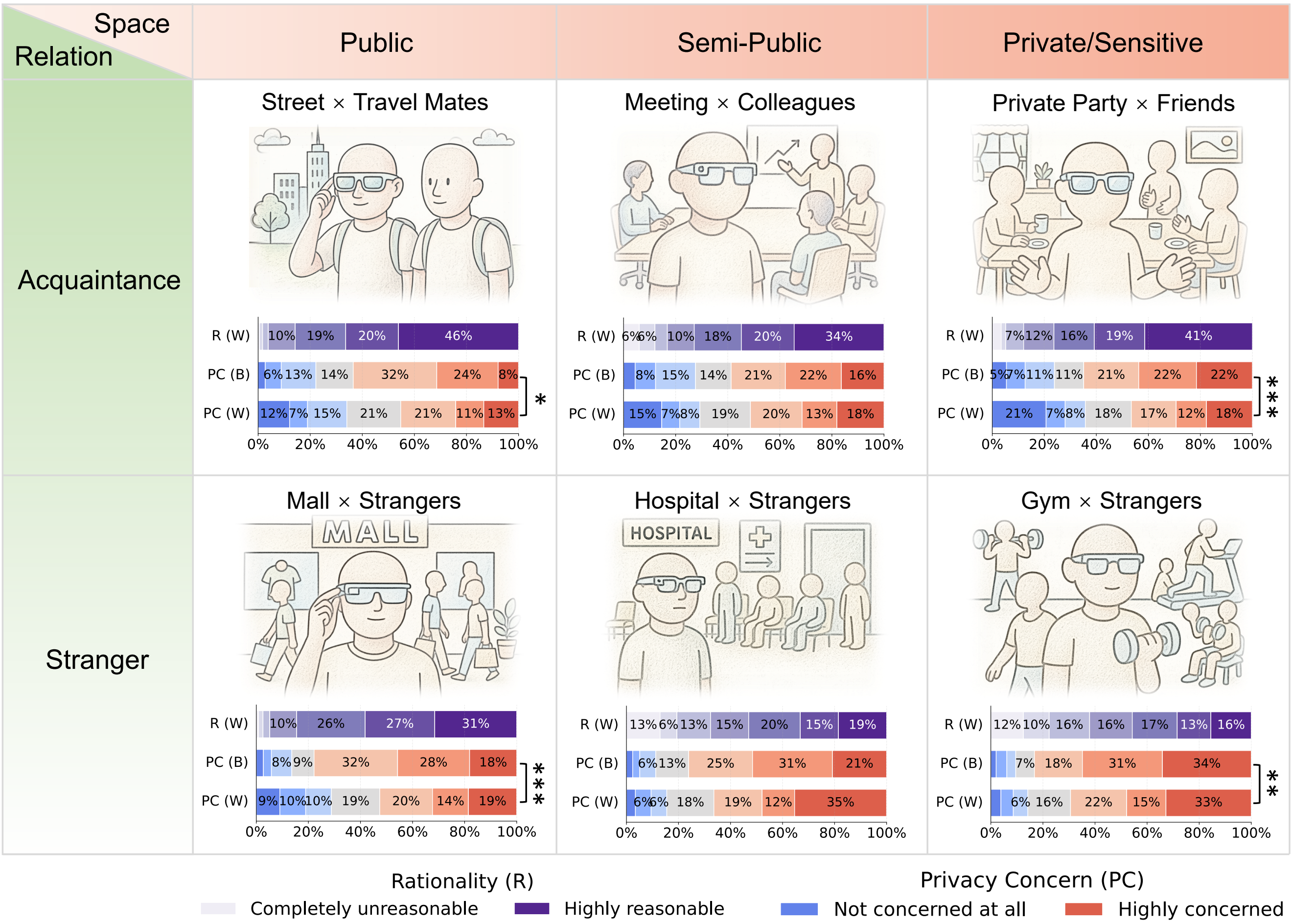

Figure 3: Privacy perceptions across six contextual scenarios. Each panel shows scenario illustration and distribution of responses for Recording Reasonability (R(W)) by wearers, Privacy Concern by bystanders (PC(B)), and Privacy Concern by wearers (PC(W)). Asterisks indicate significant group differences (* $p < .05$, ** $p < .01$, *** $p < .001$).

and Scenario (within-subjects: 6 vignettes) effects on privacy concerns, information disclosure needs/willingness, and protective measure expectations/willingness. Post-hoc comparisons used ART-C [36] with Holm corrections.

3.6 Results

3.6.1 Recording Reasonability and Privacy Concerns. Wearers consistently viewed recording as reasonable across all contexts, with mean ratings exceeding the neutral midpoint even in sensitive settings (Street × Travel Mates: $M = 5.92$, $SD = 1.26$; Gym × Strangers: $M = 4.17$, $SD = 1.94$). A significant Scenario effect ($F = 59.548$, $p < .001$) revealed clear hierarchies: public recordings with companions were deemed most reasonable, while medical and fitness contexts were least reasonable though still above neutral (Figure 3).

Bystanders expressed significantly higher privacy concerns than wearers across all scenarios ($F = 20.540$, $p < .001$; bystanders: $M = 5.07$, $SD = 1.59$; wearers: $M = 4.59$, $SD = 1.93$). Privacy-sensitive spaces—Gym × Strangers ($M = 5.46$) and Hospital × Strangers ($M = 5.26$)—triggered the highest concerns ($F = 56.440$, $p < .001$). Group × Scenario interactions revealed persistent perception gaps, with bystanders reporting significantly higher concerns in four scenarios: Street × Travel Mates ($\Delta M = 0.51$, $p < .05$), Private Party × Friends ($\Delta M = 0.79$, $p < .001$), Mall × Strangers ($\Delta M = 0.72$, $p < .001$), and Gym × Strangers ($\Delta M = 0.42$, $p < .01$). These disparities suggest wearers systematically underestimate privacy implications, particularly in social and commercial settings.

3.6.2 Behavioral Response Patterns. Bystanders demonstrated strong defensive intentions when encountering smart glasses recording (Figure 4). Camera avoidance dominated across contexts (52–80%), peaking in commercial spaces (Mall: 80%) and fitness facilities (Gym: 68%) where anonymity expectations are highest. Responses followed a clear escalation hierarchy: nonverbal protests (31–51%) served as middle ground, while direct interventions, requesting recording cessation (26–51%) or data deletion (31–39%), increased in unfamiliar settings. Formal complaints to authorities, though rare (0–13%), peaked in medical (11%) and fitness (13%) environments.

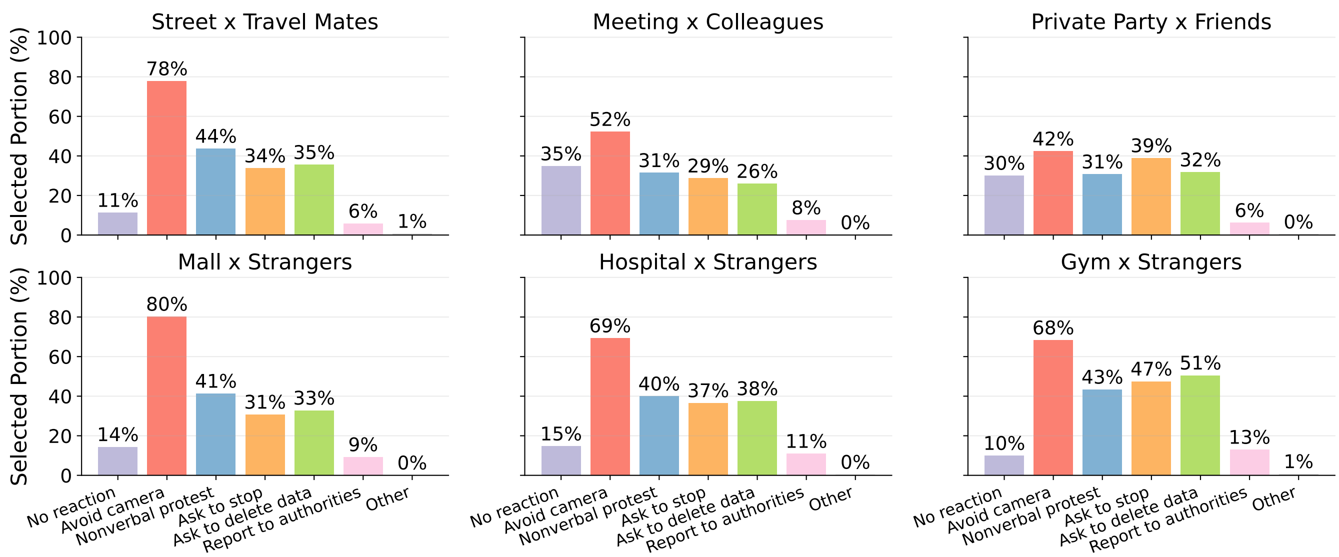

Figure 4: Bystanders' anticipated behavioral responses to smart glasses recording across six scenarios. Bars represent the percentage of participants endorsing each response option (multiple selections allowed).

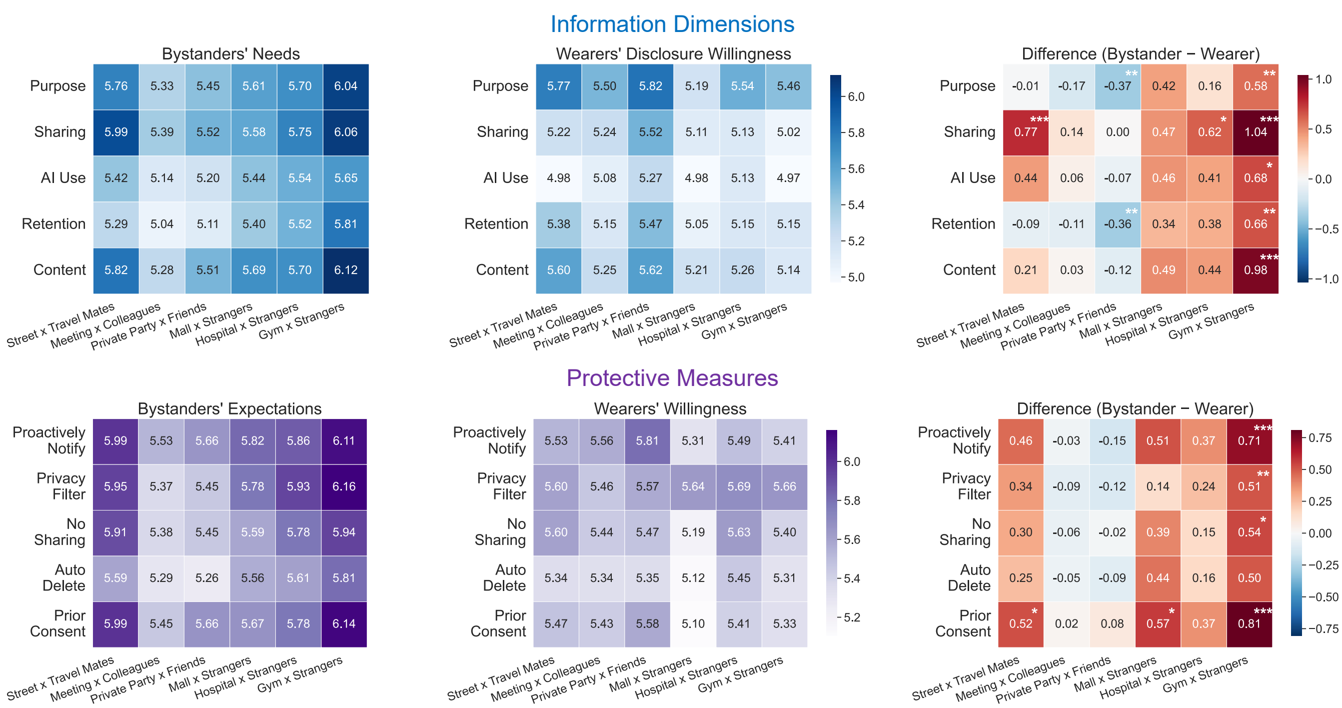

Figure 5: Information transparency and protective measure expectations across scenarios. Top row: Information dimensions. Bottom row: Protective measures. Left panels show bystanders' needs, middle panels show wearers' willingness, and right panels show the difference (Bystander − Wearer). Warmer colors indicate larger gaps. Asterisks denote significant differences (* $p < .05$, ** $p < .01$, *** $p < .001$).

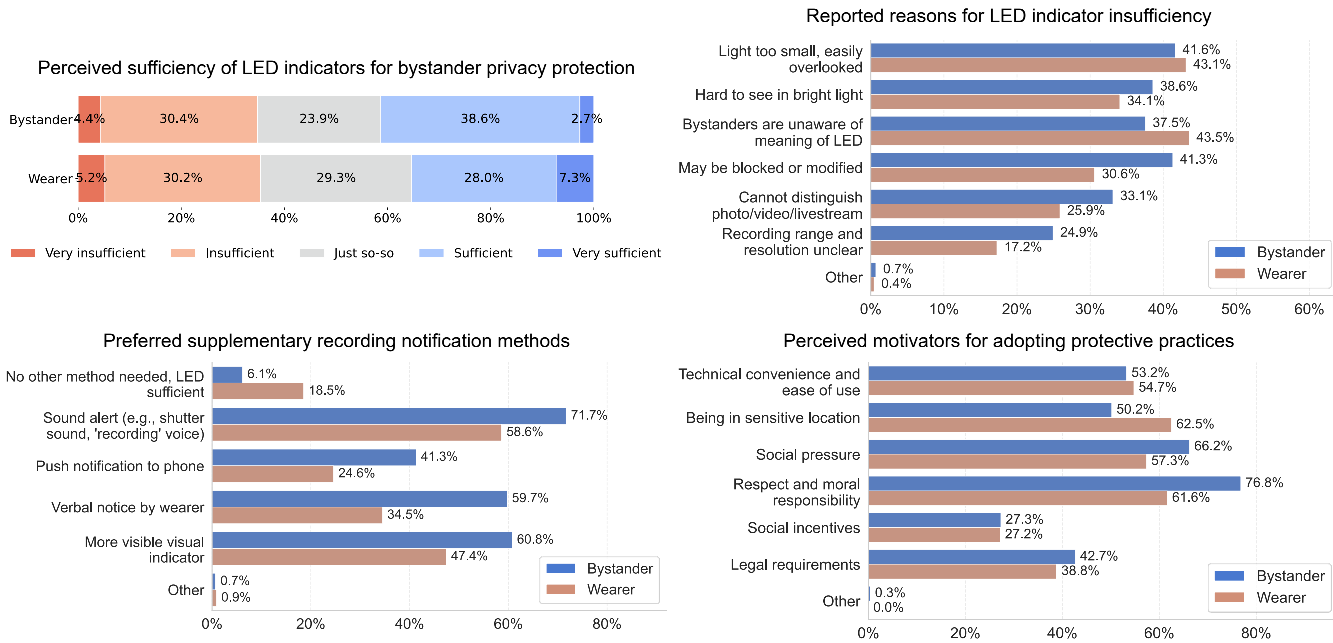

Figure 6: Evaluation of LED indicators and preferences for enhanced recording notifications. Top left: Perceived sufficiency of LED indicators. Top right: Reasons for insufficiency. Bottom left: Preferred additional notification methods. Bottom right: Perceived motivators for adopting privacy-protective practices. Blue bars represent bystanders; red bars represent wearers.

Passive acceptance remained uncommon (10–15%) except in professional settings (35%) where workplace dynamics may discourage resistance. With 65–90% of bystanders indicating they would take defensive action, these findings underscore the need for proactive privacy mechanisms that prevent rather than trigger defensive behaviors.

3.6.3 Information Transparency and Protection Expectations. Systematic gaps emerged between bystanders' expectations and wearers' willingness across information transparency and protective measures (Figure 5). Two dimensions showed significant group differences: bystanders demanded stricter **data sharing** control than wearers would provide ($F = 10.233$, $p < .01$), and **prior consent** expectations significantly exceeded wearers' willingness ($F = 7.835$, $p < .01$).

Context amplified these disparities systematically. Gym × Strangers produced the largest gaps across multiple dimensions: data sharing ($\Delta M = 1.04$, $p < .001$), recording purpose ($\Delta M = 0.58$, $p < .001$), content transparency ($\Delta M = 0.98$, $p < .001$), prior consent ($\Delta M = 0.81$, $p < .001$), and proactive notification ($\Delta M = 0.71$, $p < .001$). Hospital × Strangers showed similar patterns, while familiar settings exhibited smaller disparities. This mirrors privacy concern findings—contexts triggering heightened concerns generate demands for transparency and protection that wearers are unwilling to meet.

3.6.4 Adequacy of Current Recording Indicators. Neither stakeholder group viewed LED indicators as adequate privacy protection (Figure 6). Only 41.3% of bystanders and 35.3% of wearers considered LEDs sufficient. Participants identified critical failure modes: LEDs are too small and easily overlooked (41.6% bystanders, 43.1% wearers), become invisible in bright environments (38.6%, 34.1%), remain meaningless to unfamiliar observers (37.5%, 43.5%), and can be deliberately obstructed (41.3%, 30.6%).

Participants strongly endorsed multi-modal notification systems. Sound alerts garnered highest support (71.7% bystanders, 58.6% wearers), followed by enhanced visual indicators (60.8%, 47.4%). Role-dependent preferences emerged: bystanders favored systemic solutions like smartphone notifications (41.3% vs. 24.6%), while wearers preferred interpersonal approaches like verbal notice (59.7% vs. 34.5%). Only 6.1% of bystanders and 18.5% of wearers believed LEDs alone sufficed.

Beyond technical solutions, participants identified moral responsibility as the primary driver for privacy protection (76.8% bystanders, 61.6% wearers), followed by social pressure to avoid conflict (66.2%, 57.3%) and contextual sensitivity (50.2%, 62.5%). Legal requirements (42.7%, 38.8%) and social incentives (27.3%, 27.2%) played secondary roles, suggesting that fostering privacy-protective behaviors requires appealing to ethical sensibilities rather than regulatory compliance.

3.6.5 Role of Familiarity with Smart Glasses. To examine whether our findings are driven by participants unfamiliar with smart glasses, we analyzed how self-reported familiarity relates to scenario-averaged privacy attitudes. We conducted ANOVAs with group (bystander vs. wearer) and familiarity as factors (Figure 7).

For **privacy concern**, we observed significant main effects of group ($F(1, 503) = 14.87$, $p < .001$) and familiarity ($F(3, 503) = 9.94$, $p < .001$), and critically, a Group × Familiarity interaction

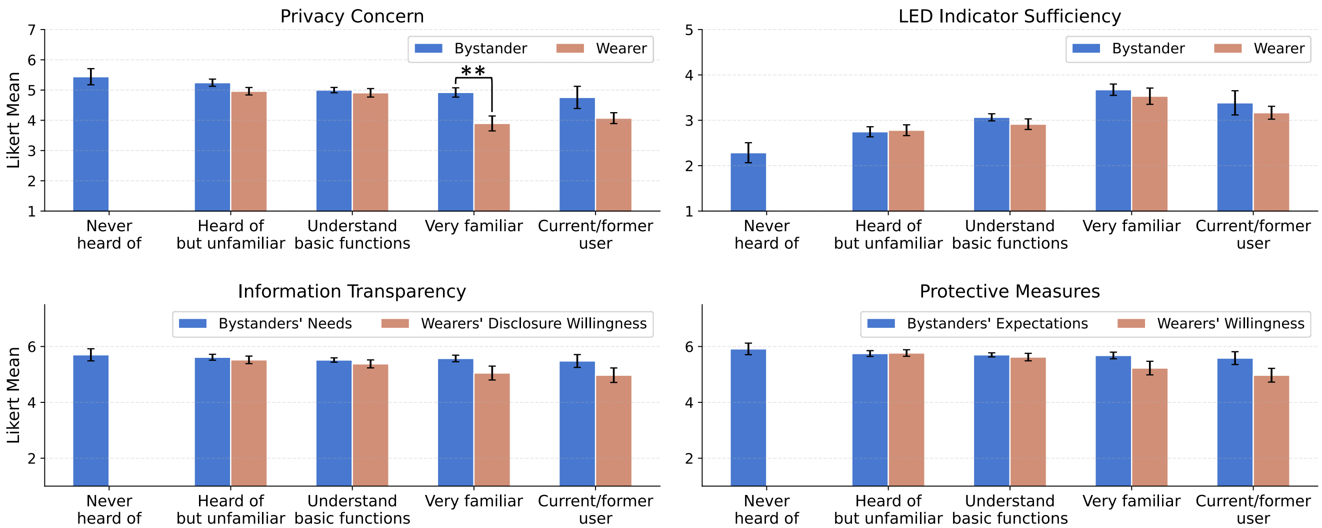

Figure 7: Effects of familiarity with smart glasses on privacy attitudes. Each panel shows mean ratings (error bars: 95% CI) for bystanders (blue) and wearers (orange) across four familiarity levels. Note: no participant in wearers group is "never heard of camera glasses".

($F(3, 503) = 3.44$, $p = .017$). Bystanders maintained consistently high concerns across all familiarity levels, while wearers' concerns decreased with experience, widening the gap between groups. For **LED sufficiency**, perceived adequacy increased with familiarity ($F(3, 503) = 8.77$, $p < .001$) but remained around the scale midpoint even among current users, with no group differences. For **information transparency** and **protective measures**, neither showed significant effects of group, familiarity, or their interaction (all $ps >$ .12).

These results demonstrate that including unfamiliar participants does not artificially inflate our findings. Bystanders' expectations remain uniformly high regardless of familiarity, while the primary effect is that experienced wearers become less concerned yet still do not view LEDs as sufficient. This reinforces our claim that privacy gaps are structural rather than artifacts of unfamiliarity, consistent with prior work showing that familiarity does not resolve privacy concerns in ubiquitous computing contexts [7].

3.7 Summary of Study 1 Findings

Our examination of privacy perceptions across six contextual scenarios reveals fundamental misalignments between stakeholder groups that illuminate why current camera glasses struggle with social acceptance.

3.7.1 RQ1: Context as Primary Determinant of Privacy Acceptability. Physical settings and social relationships emerge as primary determinants of privacy expectations, but with asymmetric effects across groups [90, 104]. Wearers maintained relatively stable perceptions of recording reasonability across all contexts (means > 4.0), operating under an assumption of general acceptability. Bystanders, however, exhibited strong contextual sensitivity: privacy-sensitive spaces triggered not only heightened concerns but also defensive behavioral intentions—up to 80% would take action in commercial and fitness contexts.

This asymmetry reveals a fundamental disconnect: wearers view context as modulating the *degree* of acceptable recording, while bystanders experience context as determining *whether* recording should occur at all. The consistency of defensive responses (65–90% across scenarios) indicates that current designs trigger conflict rather than facilitate negotiation. Privacy emerges as a situated phenomenon where spatial norms, social dynamics, and power relationships converge to define acceptable sensing practices [16, 89].

3.7.2 RQ2: The Systematic Expectation-Willingness Gap. Our findings reveal a persistent chasm between bystanders' expectations and wearers' willingness, most acute for **data sharing control** and **prior consent**, precisely the mechanisms that would provide bystanders meaningful agency [131]. The disparity intensifies in sensitive contexts where bystanders' vulnerability peaks while wearers' willingness plateaus, creating an inverse relationship that exacerbates tensions.

This gap reflects structural incompatibilities rather than inadequate goodwill. Bystanders' demands represent reasonable responses to involuntary surveillance [63, 88], while wearers' reluctance reflects practical constraints of device functionality [137]. Current notification mechanisms exemplify this incompatibility: LED indicators fail both groups—deemed inadequate by two-thirds of participants—due to limitations in perceptibility, interpretability, and circumvention resistance, consistent with prior work [58, 99].

3.7.3 Implications for Privacy Mechanism Design. The expectation-willingness gap cannot be resolved through better individual mechanisms or user education alone [121]. Contextual variation demands adaptive rather than universal approaches, while inadequate notifications reveal fundamental tensions between transparency and covert recording capabilities [60]. The prominence of moral responsibility as a motivator (outweighing technical convenience or legal requirements) suggests that effective solutions must engage ethical frameworks and social norms, pointing toward environmental protections that remove the burden from individual bystanders [1, 112].

The persistent defensive responses indicate that passive awareness mechanisms often create rather than resolve privacy conflicts, calling for a shift from post-capture remediation to prevention-oriented design. Study 2 investigates whether existing PETs can bridge these structural gaps.

4 Study 2: Evaluating Privacy-Enhancing Technologies for Camera Glasses

Study 1 revealed systematic expectation-willingness gaps between wearers and bystanders that current privacy mechanisms fail to address. Bystanders consistently demanded stronger transparency and control than wearers were willing to provide, with disparities intensifying in sensitive contexts. LED indicators failed both stakeholder groups, while defensive behavioral intentions (65–90% of bystanders) indicated that current approaches generate rather than resolve privacy conflicts.

These findings raise critical questions about whether existing Privacy-Enhancing Technologies (PETs) can bridge these structural misalignments. To investigate this, Study 2 evaluates twelve representative PETs through paired interviews combining HCI researchers/designers (who contribute theoretical expertise) with experienced smart glasses users (who provide practical insights). This dyadic approach enables assessment of both technical feasibility and real-world viability. Study 2 addresses two research questions:

- **RQ3: Context-Dependent Viability.** Can PETs adapt to the contextual variation in privacy needs identified in Study 1, or are new paradigms necessary?
- **RQ4: Effectiveness-Usability Trade-offs.** Do current PETs successfully balance privacy protection with practical usability?

4.1 PET Selection and Classification

We conducted a literature review following PRISMA guidelines [92] to identify privacy protection mechanisms for bystanders across camera glasses, AR/VR devices, and smart home technologies. We queried SCOPUS, ACM Digital Library, and IEEE Xplore, targeting premier HCI venues (CHI, IMWUT, CSCW), AR/VR conferences (IEEE VR, ISMAR), and privacy forums (IEEE S&P, SOUPS, PoPETs). Using keywords related to bystander privacy, wearable cameras, and privacy-enhancing technologies, we identified 127 unique records. Two researchers independently screened papers based on: (1) explicit bystander privacy focus, (2) proposed technical mechanisms, and (3) wearable camera relevance. This yielded 70 relevant papers, supplemented by commercial implementations from Snap Spectacles, Ray-Ban Meta, and Apple Vision Pro (Cohen's $\kappa = 0.83$).

Through thematic synthesis [122] and reference to existing taxonomies [28, 94], we organized PETs into four functional categories:

- **Wearer-side Awareness Mechanisms (W):** Signal recording status through visual, auditory, or digital channels
- **Bystander-side Consent Mechanisms (B):** Enable privacy preference expression through gestures, markers, broadcasting, or negotiation platforms
- **Context-aware Automatic Processing (C):** Automatically protect privacy through face anonymization or location-based restrictions
- **Platform-level Accountability Systems (P):** Ensure traceability through watermarking and post-hoc notifications

We selected 12 representative PETs spanning all categories with varying implementation complexity (Table 2). Selection prioritized: (1) comprehensive category coverage, (2) existence of functional prototypes or commercial deployments, and (3) potential to address the expectation-willingness gaps identified in Study 1.

4.2 Participants and Procedure

We recruited 20 participants forming 10 dyadic pairs (Table 3): 10 HCI researchers/designers with privacy and wearable technology expertise, and 10 camera glasses users with at least three months of device experience (recruited from Study 1 respondents). This pairing enables evaluation from both theoretical and practical perspectives. Sessions lasted approximately two hours with $30 USD compensation.

Each session followed a four-phase protocol. In **Phase 1** (~10 min), facilitators introduced study objectives and established rapport through warm-up questions. In **Phase 2** (~60 min), participants examined 12 PETs supported by textual descriptions, literature images, scenario diagrams, and UI prototypes (see supplementary materials). Each participant independently rated mechanisms on four 7-point dimensions: *Privacy Protection Effectiveness*, *User Experience and Convenience*, *Transparency and Trust*, and *Social Acceptability and Scalability*. Dyads then discussed evaluations and proposed improvements; presentation order was randomized. In **Phase 3** (~40 min), participants re-evaluated PETs across three environmental categories (public, semi-public, private/sensitive spaces) using scenario cards, ranking mechanisms by contextual suitability. **Phase 4** (~10 min) captured additional insights through synthesis and reflection.

The study protocol was reviewed and approved by the Institutional Review Board (IRB) of Tsinghua University, and we strictly protected participants' data privacy throughout the study.

4.3 Analysis

Interview recordings were transcribed verbatim and analyzed using grounded theory principles [78]. Two researchers independently conducted open coding [18] to identify emergent themes around PET effectiveness, usability concerns, contextual appropriateness, and implementation barriers. Through iterative review, we developed a codebook (see supplementary materials) and re-analyzed transcripts using axial coding [77] to examine patterns across dyads. Inter-rater reliability achieved Cohen's $\kappa = 0.79$, with disagreements resolved through discussion.

Table 2: Privacy-Enhancing Technologies (PETs) Evaluated in Study 2

Category	PET Name	Description	Literature Examples
Wearer-side Awareness (W)	W1: LED Ring Indicator	Circular LED array around camera lens; different colors indicate recording modes (white: video, green: AI, orange: livestream).	Snap Spectacles [49]; Visual indicators [3, 16, 20, 58]
	W2: Audio Alerts	Speaker emits shutter sounds for photos and verbal announcements for videos.	Korean camera standard [108]; Privacy Speaker [121]
	W3: External Display	Front-facing e-ink or LED display showing recording status to bystanders.	Apple Vision Pro EyeSight [48]; MirrorCam [57]; EyeCam [120]
	W4: Proximity Broadcast	Glasses broadcast recording status via BLE/WiFi to nearby smartphones.	WiFi notifications [97]; BLE transparency [37]; PriView [100]
Bystander-side Consent (B)	B1: Gesture Recognition	Camera recognizes standardized gestures: open palm (stop) or thumbs-up (consent).	Social signal detection [55, 80]; Gesture opt-out [9, 113]
	B2: Wearable Markers	Bystanders wear IR emitters, QR-coded clothing, or ultrasonic beacons signaling "do not record."	FacePET [96]; Visual tags [19]; Beacons [13, 68]
	B3: Preference Broadcasting	Smartphone app broadcasts privacy preferences via BLE to nearby devices.	I-Pic [2]; Cardea [112]; iRYP [118]; Do Not Capture [102]
	B4: Negotiation Platform	Real-time permission requests sent to bystander phones with allow/deny options.	Erebus [54]; Interactive negotiation [65, 142]
Context-aware Automatic Processing (C)	C1: Face Anonymization	AI-powered detection automatically blurs unauthorized faces during recording.	Bystander detection [43]; BystandAR [24]; PrivacEye [116]
	C2: Geofencing Control	GPS/WiFi-based system automatically disables recording in sensitive zones.	PlaceAvoider [119]; World-driven access [110]
Platform Accountability (P)	P1: Digital Watermarking	Recording embeds immutable watermarks with device ID and timestamp.	Geo-tagged media [45]
	P2: Face Matching	Platforms notify pre-registered users when their faces appear in uploaded content.	HideMe [66]; Cloak [112, 139]

Table 3: Study 2 Participant Demographics. Exp. = years of experience (HCI) or duration of device usage (Users).

S.	HCI Researcher/Designer (H)					Camera Glasses User (U)				
	PID	Age	Gen.	Specialization	Exp.	PID	Age	Gen.	Occupation	Exp.
1	PH1	25	M	HCI Research	2y	PU1	41	M	Business Manager	9mo
2	PH2	27	M	Usable Privacy	3y	PU2	27	M	Business Manager	1y
3	PH3	23	F	HCI Design	1y	PU3	29	M	Business Manager	1.5y
4	PH4	23	F	HCI Design	5y	PU4	30	F	Company Employee	3mo
5	PH5	23	F	HCI Design	4y	PU5	20	M	Company Employee	2mo
6	PH6	24	F	Usable Privacy	3y	PU6	29	F	Business Manager	7mo
7	PH7	22	F	HCI Research	2y	PU7	23	M	Company Employee	6mo
8	PH8	23	F	HCI Research	2y	PU8	33	M	Civil Servant	3mo
9	PH9	21	M	Usable Privacy	3y	PU9	30	M	Business Manager	6.5y
10	PH10	28	F	Platform Accountability	4y	PU10	28	M	Graduate Student	3mo

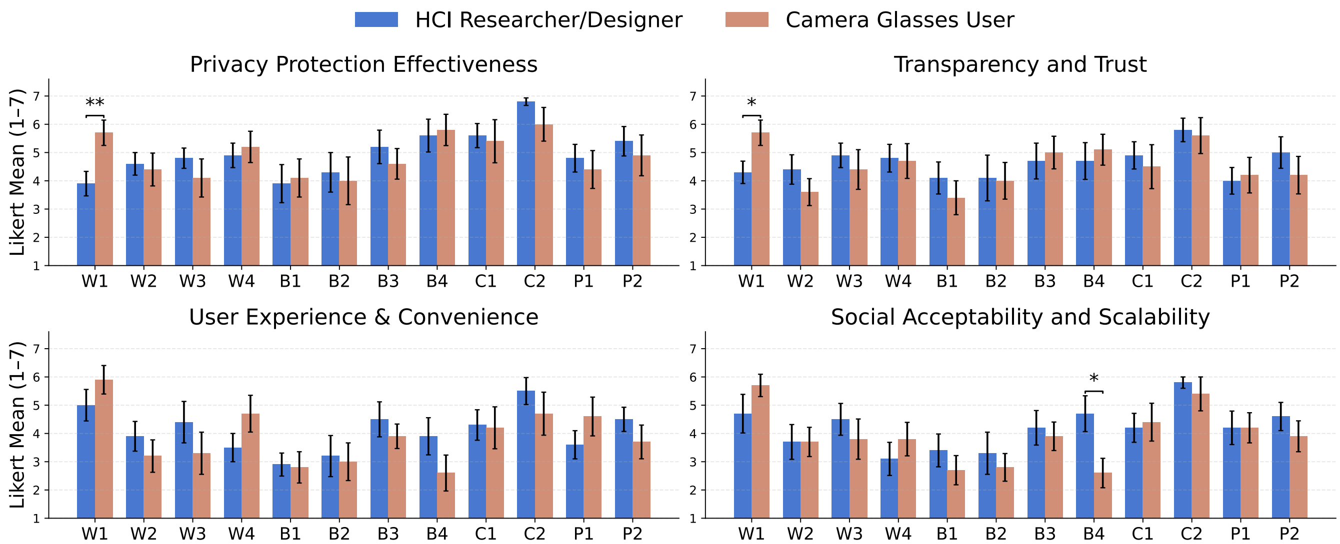

Figure 8: Comparative evaluation of 12 PETs by HCI researchers/designers (blue) and camera glasses users (red) across four dimensions. Error bars represent standard error. Asterisks indicate significant differences between groups (* p<.05, ** p<.01).

4.4 Overview of PET Evaluation Results

Quantitative ratings across four evaluation dimensions reveal distinct category-level performance patterns and systematic stakeholder differences (Figure 8).

Context-aware automatic processing (C1-C2) achieved the highest ratings across nearly all dimensions. Geofencing Control (C2) received exceptional privacy protection scores (HCI: M=6.8, Users: M=6.0), substantially outperforming all other mechanisms. Face Anonymization (C1) also performed strongly (HCI: M=5.6, Users: M=5.4), though with moderate usability concerns.

Wearer-side awareness mechanisms (W1-W4) showed mixed reception. Users rated LED Ring Indicator (W1) favorably, while HCI researchers expressed skepticism about their effectiveness (M=3.9 vs. M=5.7, p<.01). Audio Alerts (W2) and External Display (W3) received consistently mediocre ratings.

Bystander-side consent mechanisms (B1-B4) revealed fundamental trade-offs. Negotiation Platform (B4) achieved strong privacy protection scores (HCI: M=5.6, Users: M=5.8) but received the lowest usability ratings (Users: M=2.6). Gesture Recognition (B1) and Wearable Markers (B2) faced both effectiveness and acceptability challenges.

Platform-level accountability systems (P1-P2) received moderate ratings, suggesting perception as complementary rather than primary solutions.

Both groups generally agreed on relative mechanism rankings, yet notable divergences emerged. Users exhibited greater confidence in LED indicators, which HCI researchers deemed insufficient. For transparency and trust, users consistently rated awareness mechanisms higher (W1: M=5.7 vs. M=4.3, p<.05). Social acceptability ratings diverged most for negotiation platforms (B4: M=4.7 vs. M=2.6, p<.05). These patterns suggest that automated context-aware systems provide the optimal protection-usability balance, while consent mechanisms face adoption barriers despite privacy benefits.

4.5 Context as Primary Determinant of PET Selection (RQ3)

Physical and social context emerged as the primary determinant of privacy mechanism preferences, overriding individual and role-based differences. Participants systematically prioritized different mechanism categories based on environmental characteristics (Figure 9).

4.5.1 Public Spaces: Minimal-Friction Visibility. Public environments generated remarkable convergence around passive visibility mechanisms. LED Ring Indicator (W1) achieved 80% selection rates across both groups. This reflected practical scalability constraints: *"In public places, visible indicators are sufficient. Other complex mechanisms have costs that are too high...there are just too many people"* (PH10). Interactive consent mechanisms faced systematic rejection, with gesture recognition receiving 0% selection from users: *"Actively requesting permission from everyone is just not practical"* (PU10). Face Anonymization (C1) emerged as the preferred complement (70% HCI selection), addressing incidental capture through automatic rather than individual protection.

4.5.2 Semi-Public Spaces: Structured Negotiation. Professional and institutional environments created different preference patterns. Audio Alerts (W2) gained acceptance (50% HCI selection): *"In smaller scenarios involving personal privacy, voice announcements work for both parties"* (PH1). Negotiation Platform (B4) and Preference Broadcasting (B3) achieved higher support, reflecting the feasibility of structured consent in bounded environments where explicit communication is socially expected.

Figure 9: Context-dependent privacy mechanism preferences across public, semi-public, and private spaces. Each point represents one mechanism positioned by average rank (x-axis) and selection popularity (y-axis). Bubble size indicates the proportion of participants ranking it in their top three.

4.5.3 Private/Sensitive Spaces: Automated Protection. Private contexts revealed distinctions between trust-based gatherings and vulnerability-based sensitive spaces. For home gatherings, participants relied on social relationships: *"Among friends, filming is no big deal...if someone has malicious intent, they're just not my friend anymore"* (PH2). However, sensitive spaces (gyms, changing rooms) triggered strong preferences for automated protection. Geofencing Control (C2) achieved its highest selection rates (60-70%): *"For situations involving body exposure, automatic shutdown is best, regardless of who's filming"* (PU2). This vulnerability-based reasoning prioritized comprehensive protection over user autonomy in high-stakes contexts.

4.6 Fundamental Trade-offs in Current PETs (RQ4)

Our evaluation revealed four fundamental trade-offs that undermine current PET approaches, explaining why no single mechanism category can reconcile the stakeholder conflicts identified in Study 1.

4.6.1 Visibility vs. Disruption. Awareness mechanisms (W1-W4) face an irreconcilable tension: mechanisms sufficiently noticeable to inform bystanders inevitably disrupt social interactions, while subtle approaches fail to provide meaningful transparency.

LED indicators exemplify this contradiction. Users viewed dynamic lighting as intuitive: *"You immediately sense these are electronic glasses"* (PU10). However, researchers identified critical limitations: environmental dependency (imperceptible in bright daylight), lack of standardization across products, and circumvention vulnerability: *"Just physically block it...two millimeters of tape, algorithms can't detect it"* (PH4). This "deters the honest but not the malicious" nature undermines protection purposes.

Audio Alerts (W2) and External Display (W3) attempted to address visibility limitations but introduced severe social friction. Audio notifications faced rejection: *"This is so awkward...suddenly a loud voice during photography"* (PU10). External displays offered clarity but at aesthetic cost: *"It affects appearance so much I wouldn't buy it"* (PU3). Proximity Broadcast (W4) achieved highest privacy protection scores (5.05/7) but lowest social acceptability (3.45/7), with industry insiders noting that phone manufacturers would block such functionality (PU9). Even successful implementation wouldn't solve the core issue: *"What's the point of awareness? I know, but can I stop it?"* (PU4).

4.6.2 Empowerment vs. Burden. Consent mechanisms (B1-B4) suffer from a fundamental paradox: empowering bystanders requires burdening them with responsibilities that should belong to those creating privacy risks.

Participants identified the injustice of requiring potential victims to actively defend themselves. For Gesture Recognition (B1): *"The responsibility for privacy invasion lies with the recorder, but now you're making the recorded party perform gestures...transferring the burden to the victim"* (PU8). This sentiment intensified with Wearable Markers (B2): *"It's like victim-blaming...the fundamental problem lies with those creating danger"* (PH3).

App-based mechanisms (B3-B4) offered sophisticated control but with severe practical costs: platform fragmentation, battery drain, and exclusion of populations without smartphones. Negotiation Platform (B4) achieved strong privacy scores (5.8/7) but lowest usability ratings (2.6/7): *"If I encounter 100 people at a tourist site, I'd have to communicate with all 100. The moment I wanted to capture would be gone"* (PU10). The enforcement dilemma proved critical: mandatory enforcement eliminates user discretion, while optional compliance becomes merely symbolic. Direct interpersonal communication consistently emerged as preferred: *"Just tell the glasses wearer 'don't record me,' isn't that better?"* (PU1).

4.6.3 Protection vs. Agency. Automated processing mechanisms (C1-C2) received highest privacy ratings yet create conflicts between protection goals and user autonomy.

Face Anonymization (C1) appealed conceptually but faced implementation challenges. Computational constraints proved significant: *"Currently I can only record four 10-minute videos before battery death. Adding real-time blurring would reduce this further"* (PU6). The mechanism also cannot solve identification problems: *"I might think I'm filming this handsome guy but actually have him off to the side while recording the pretty girl in the center. Who gets blurred?"* (PU9).

Geofencing Control (C2) achieved highest ratings overall (Privacy Protection: Users 6.0, HCI 6.8) but faces technical barriers: GPS cannot distinguish floors, WiFi connectivity is limited, and computational demands would reduce battery life dramatically. Philosophical disagreements emerged, with some participants viewing mandatory restrictions as *"deliberately crippled products"* while others saw them as embedding legal compliance. Both mechanisms struggled with contextual nuance, as artistic and documentation needs clashed with blanket restrictions. A critical weakness emerged around transparency: *"The person being recorded still doesn't know about processing...they would still feel uncomfortable"* (PH7). However, the high ratings for geofencing despite implementation challenges reveal acceptance of reduced functionality when privacy stakes are highest: *"Some places absolutely shouldn't allow recording, like bathrooms, and this should apply universally"* (PH6).

4.6.4 Accountability vs. Exposure. Platform-level mechanisms (P1-P2) attempt deterrence through post-capture consequences but require surrendering privacy to protect it.

Digital Watermarking (P1) requires mandatory real-name authentication and device binding, creating surveillance infrastructure: *"If this mechanism existed, I probably wouldn't buy the device. It violates the recorder's rights while protecting the recorded person"* (PU8). Face Matching (P2) exemplified this paradox more starkly: *"You're building an extremely dangerous dataset to solve problems that may not even exist yet"* (PH2). Users must upload biometric data to platforms they don't trust, exposing themselves to risks potentially exceeding those they seek to avoid.

Both mechanisms faced scalability barriers and neither prevents initial violations, only offering potential post-hoc recourse. The moderate ratings (3.9-5.4) reflect recognition of deterrence value tempered by severe concerns about privacy surrenders and platform dependencies required for implementation.

5 Context-Adaptive Privacy Pathways for Camera Glasses

Through two complementary studies examining privacy negotiation from multiple stakeholder perspectives across diverse contexts, our work offers a systematic account of how privacy expectations diverge and how PETs succeed or fail under different conditions. In this section, we translate these insights into context-adaptive design framework and discuss potential pathways for future PET development. We emphasize that these pathways represent a proposed design framework grounded in our empirical findings rather than a validated system implementation.

5.1 Key Patterns for Context-Adaptive Design

Our studies reveal three key patterns that inform context-adaptive design.

Asymmetric contextual sensitivity. Wearers and bystanders exhibit fundamentally different relationships with context. Wearers maintained relatively stable recording reasonability perceptions across all scenarios (means > 4.0), treating context as modulating the *degree* of acceptable recording. Bystanders showed dramatic contextual variation ($F = 56.440$, $p < .001$), with sensitive contexts generating nearly 2-point higher concerns than public settings. This asymmetry reveals a fundamental disconnect: wearers view context as adjusting "how much" disclosure is needed, while bystanders experience context as determining "whether" recording should occur at all.

Gap concentration in control dimensions. Expectation-willingness gaps systematically amplify in scenarios characterized by vulnerability. Gym × Strangers produced the largest disparities across data sharing ($\Delta M = 1.04$), prior consent ($\Delta M = 0.81$), and content transparency ($\Delta M = 0.98$). Critically, these gaps concentrate in control dimensions (consent, data sharing) rather than transparency dimensions (purpose disclosure: $\Delta M = 0.58$). This suggests that awareness-centric approaches, which dominate current designs, address secondary rather than primary privacy needs. As one participant noted: *"What's the point of awareness? I know, but can I stop it?"* (PU4).

Context-specific mechanism acceptance. Study 2 revealed that stakeholder convergence emerged *within* contexts but diverged

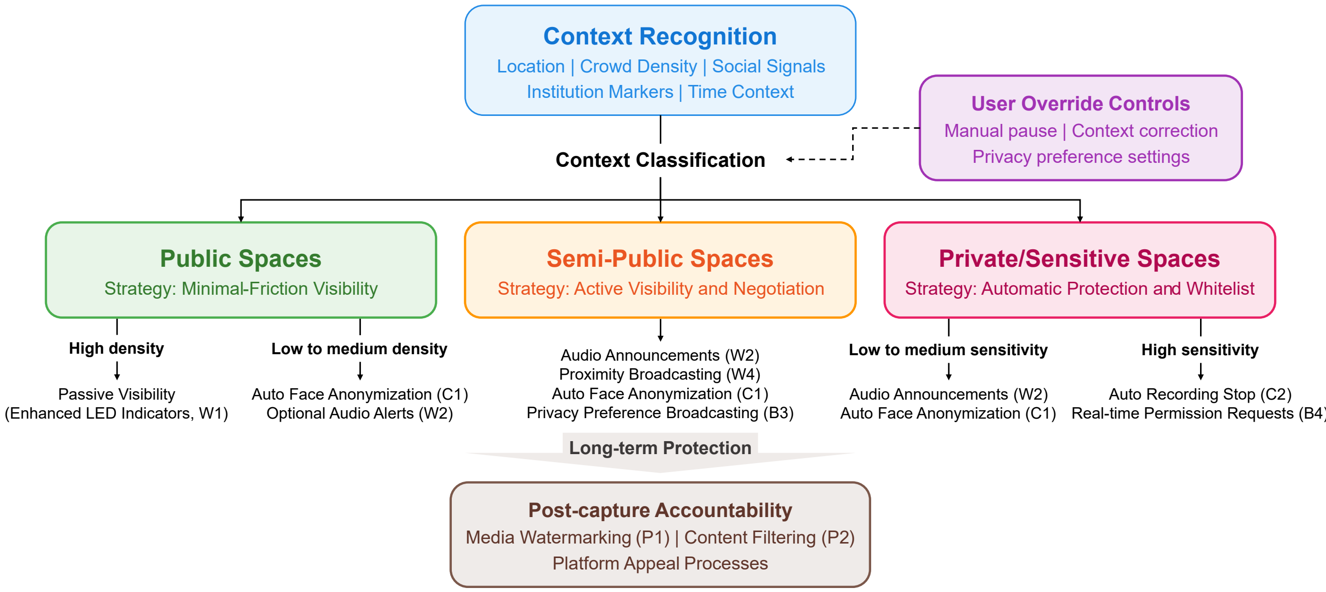

Figure 10: Proposed context-adaptive privacy protection pathways for camera glasses. The system recognizes contextual characteristics, classifies environments into primary categories, and deploys appropriate mechanism combinations while preserving user override controls.

across contexts. Public spaces saw 80% convergence on passive visibility, with interactive consent receiving 0% user selection. Semi-public spaces enabled negotiation platforms that were rejected elsewhere. Sensitive spaces triggered strong preferences for automatic protection (60–70% selection), with participants prioritizing comprehensive protection over user autonomy. These patterns indicate that effective privacy protection requires adaptive strategies calibrated to environmental and social characteristics rather than universal solutions.

5.2 Proposed Context-Adaptive Pathways

The fundamental trade-offs revealed across PET categories (visibility versus disruption, empowerment versus burden, protection versus agency, accountability versus exposure) demonstrate that static, universal mechanisms cannot achieve effective privacy protection. Based on our findings, we propose a context-adaptive framework operating on three core pathways (Figure 10).

Environmental recognition identifies contextual characteristics through location data, crowd density estimation, institutional markers, and temporal patterns without invasive monitoring. **Dynamic strategy selection** deploys distinct protection approaches: public spaces activate minimal-friction visibility (W1) with optional face anonymization (C1); semi-public environments enable structured negotiation through audio announcements (W2) and preference broadcasting (B3); sensitive spaces trigger automatic recording restrictions (C2) or permission-based access (B4). **Layered protection** maintains baseline protections universally while activating context-triggered mechanisms and preserving user override capabilities [61].

These adaptive pathways addresses the fundamental trade-offs identified in our analysis. The visibility contradiction resolves through context-appropriate notification intensity. The control dilemma transforms from universal burden to selective empowerment, with bystanders gaining automatic protections in vulnerable contexts rather than requiring constant self-defense. The automation challenge becomes contextually bounded, preserving user agency in public spaces while accepting intervention where vulnerability justifies reduced control.

5.3 Illustrative Application Scenarios

To demonstrate the applications of context-adaptive pathways, we constructed three representative scenarios across public, semi-public, and sensitive environments. These scenarios track Information Transparency (IT) and Protective Measures (PM), the two dimensions where expectation-willingness gaps were most pronounced, illustrating how each pathway dynamically adjusts protection strategies in response to evolving contextual cues.

5.3.1 Public Space: Vlogger in a Park. Figure 11 illustrates a vlogger recording while jogging. When the wearer activates recording, both IT and PM decline as bystanders face uncertainty about capture status. The system detects recording activation and recommends enhanced LED ring indicators (W1) with semantically meaningful states (white for recording, green for AI processing, red for livestreaming), stabilizing IT and modestly improving PM. As crowd density increases and more identifiable faces appear, contextual recognition updates its assessment and activates automatic face anonymization (C1), substantially raising PM while maintaining stable IT. Without these interventions (dashed curves), both metrics would continue deteriorating.

5.3.2 Semi-Public Space: Office Meeting. Figure 12 depicts an employee capturing meeting notes. Colleagues share a virtual workspace

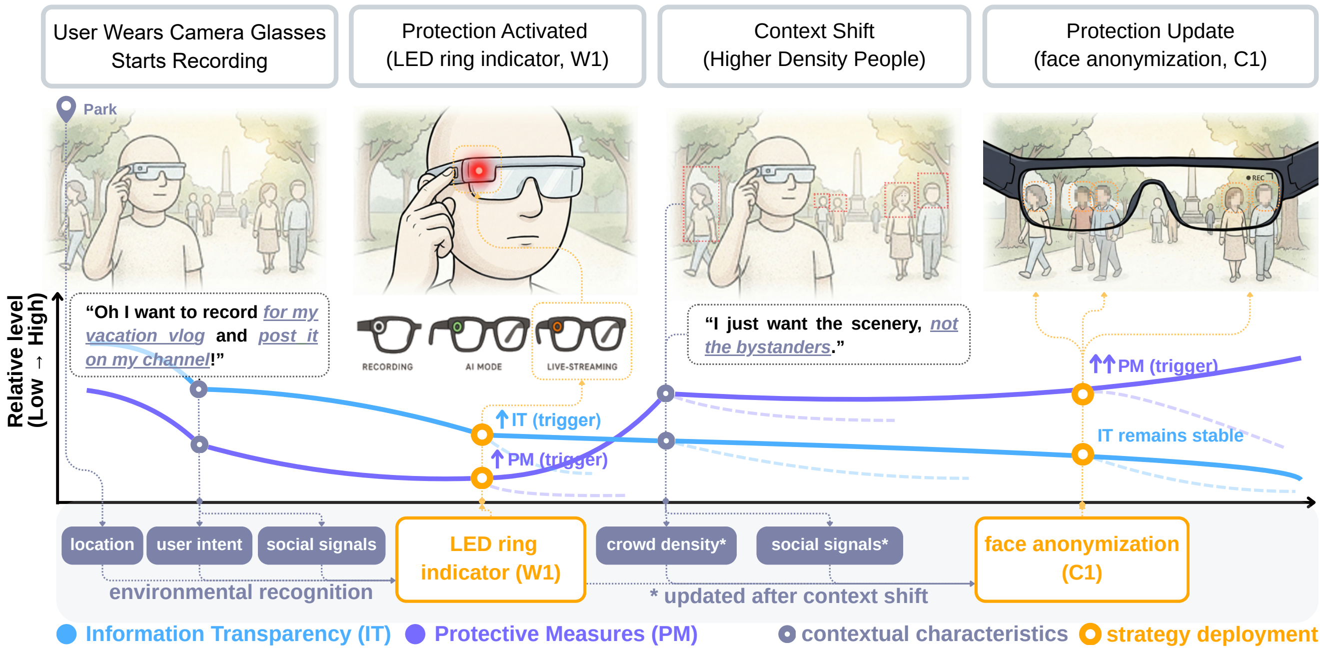

Figure 11: Context-adaptive privacy protection for a vlogger in a public park. The system adjusts strategies as contextual cues evolve: enhanced LED ring indicators (W1) stabilize IT when recording begins, and face anonymization (C1) raises PM as crowd density increases. Dashed curves show trajectories without intervention.

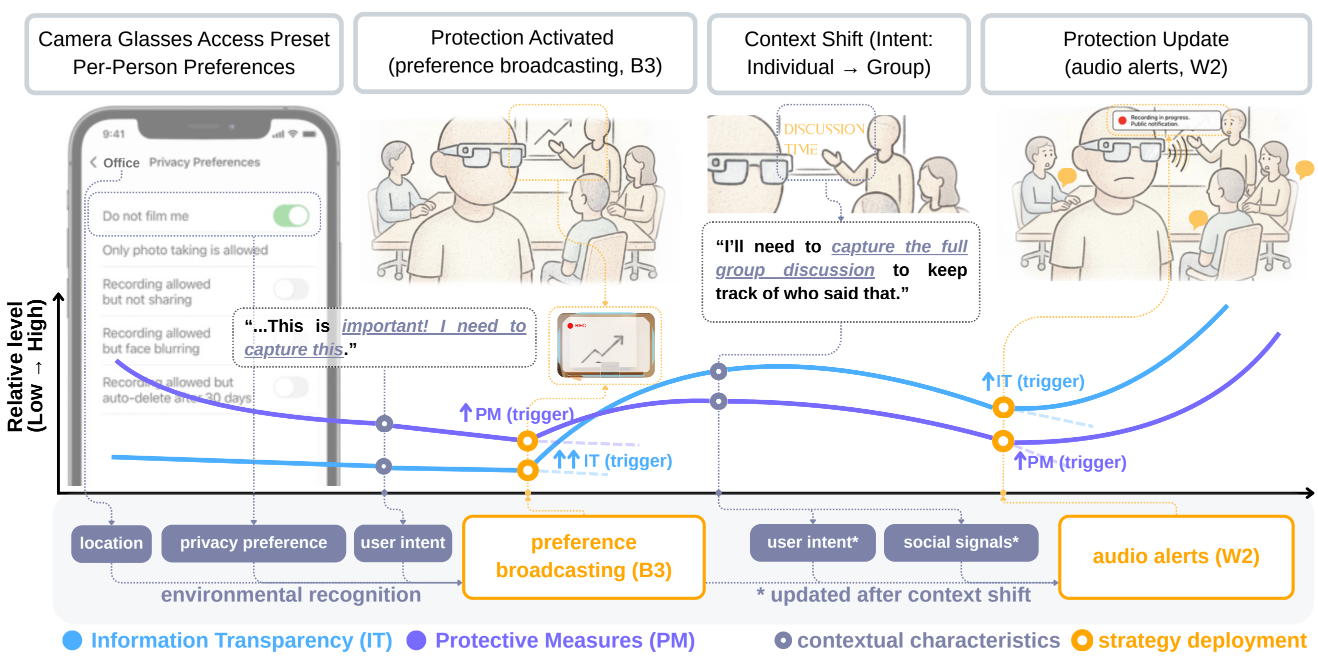

Figure 12: Context-adaptive privacy protection during an office meeting. Preset preferences enable proximity broadcasting (B3); explicit consent requests trigger audio alert (W2) when recording scope expands.

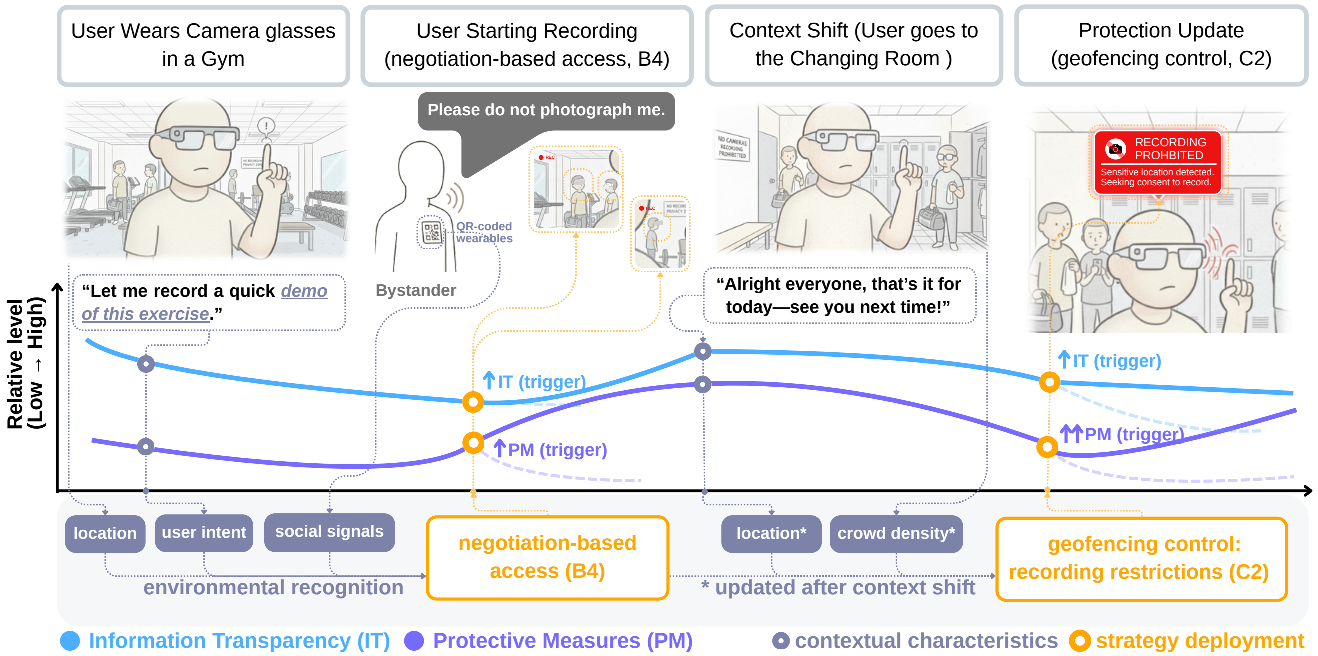

Figure 13: Context-adaptive privacy protection in a gym. Face anonymization via negotiation-based access (B4) activates when opt-out markers are detected; automatic geofencing control (C2) triggers upon entering the changing room.

where they pre-configure privacy preferences (e.g., "Do not film me," "Photo only"). These preferences are automatically broadcast to nearby devices as the meeting begins.

When the wearer decides to capture the whiteboard, the system triggers proximity broadcasting (B3) based on the preset preference as the recommended protection. Since this aligns with default permissions, no explicit negotiation is required, and IT and PM stabilize. Later, when the wearer requests to capture the group discussion itself, contextual recognition detects this intent shift and activates consent-based audio alerts (W2). IT rises as everyone receives clear notification, while PM increases as colleagues can adjust their positions or explicitly consent.

5.3.3 *Sensitive Space: Gym and Changing Room.*

Figure 13 follows a fitness instructor recording an exercise demonstration. When recording begins, IT and PM decline as the action introduces potential incidental capture. As individuals with opt-out markers (e.g., QR-coded wearables) enter the frame, the system activates contextual face anonymization via negotiation-based access (B4), thereby stabilizing IT and raising PM.

When the instructor finishes the livestreaming sessions and enters the changing room, contextual recognition detects transition into a highly sensitive location. The system triggers geofencing control (C2) — an automatic recording shutdown, producing a sharp PM increase as mandatory restrictions take effect in protected spaces. This scenario illustrates how adaptive systems can enforce graduated protection, from voluntary anonymization in general gym areas to mandatory cessation in spaces where vulnerability justifies overriding user autonomy.

Together, these scenarios illustrate how context-adaptive pathways can dynamically mediate the expectation-willingness gap by selecting appropriate protection strategies based on environmental characteristics, user intent, and bystander signals.

5.4 Implementation Challenges and Future Directions

Realizing context-adaptive privacy requires coordination across technical, regulatory, and social dimensions. As one participant noted, *"Many issues aren't things a single manufacturer can solve—they involve upstream and downstream platforms, government policies, and user education"* (PH10).

Near-term enhancements should focus on improving current mechanisms. Passive indicators (W1) will likely remain the most accepted notification form but must evolve beyond theatrical compliance. Transparent hardware design should replace concealed recording [58], and manual camera covers can provide tangible trust signals [31]. Multi-modal feedback (enhanced LED visibility, selective audio cues, haptic confirmation) can address situational constraints while minimizing disruption [3, 137]. Hybrid approaches combining user input with automated detection may address the algorithmic difficulty of distinguishing subjects from bystanders [87, 116, 131].

Medium-term development should pursue context-adaptive systems. Binary recording approaches should give way to graduated protection levels [26]: original capture for trusted contexts, aesthetic-preserving filters for public spaces, complete restriction for sensitive areas. Such adaptive defaults are critical since users rarely modify initial configurations [1]. Location, social density, and institutional cues can inform automatic adjustments, while contextual preference prediction [138] may reduce user burden. Lightweight negotiation protocols prioritizing immediacy, such as gesture-based responses [14] or pre-configured permissions [2, 112], can support ephemeral encounters.

Long-term ecosystem development requires industry standardization elevating privacy protection from user discretion to system-level enforcement [124], specifying minimum notification requirements and cross-manufacturer interoperability. Regulatory frameworks must address ubiquitous sensing devices specifically, moving beyond traditional consent models toward environmental protection standards. Social norm development must complement technical measures [16, 89], with public education establishing expectations for voluntary restraint in sensitive contexts and organizations developing clear camera-glasses policies.

These efforts collectively mark a shift from binary privacy approaches toward contextually intelligent systems that recognize privacy as dynamically shaped by environmental and social characteristics.

6 Discussion

6.1 Contextual Asymmetry in Privacy Negotiation

Context emerged as the primary determinant of privacy acceptability in both studies. Study 1 showed that physical settings and social relationships intensify the expectation-willingness gap, highlighting context as a fluid, co-constructed frame that shapes how people interpret capture [61, 131]. Because camera-glasses privacy centers on whether sensing should occur rather than how information flows afterward, our findings extend classic privacy models from static information management toward ongoing contextual negotiation [11, 86]. Study 2 further demonstrates that PET preferences shift with these contextual interpretations, underscoring the need for adaptive pathways that accommodate evolving notions of context and agency.

Our findings also surface additional contextual layers that influence capture judgments. Behavioral cues such as gesture, intent, timing, and framing [40, 55, 114] actively reshape how a setting is perceived. For example, the same classroom may feel public or private depending on what is being recorded and the wearer's visible behavior. Interface-level cues, including visual changes or capture-mode indicators [105, 131], can guide how people make sense of sensing in the moment. Personal differences including cultural norms [41, 109], accessibility needs [4, 141], and individual traits [34] create further opportunities for systems to refine contextual awareness and provide more equitable protection.

Rather than exhaustively modeling every contextual factor, our contribution lies in revealing how these elements gain significance in lived experience. By grounding privacy negotiation in situated user interpretation rather than optimization metrics [103], we point toward adaptive mechanisms that evolve with social interaction and contextual meaning.

6.2 Device Familiarity and Social Acceptance

Although familiarity was not the dominant determinant of privacy judgments, it shaped how participants evaluated camera-glasses acceptability. Increasing familiarity was associated with reduced privacy concern and lower demands for transparency, consistent with technology-familiarity and social-acceptance models [21, 29]. Professional settings amplified this effect, where normative expectations of documentation generated substantially higher passive acceptance (35%) than other contexts (10–15%). These patterns suggest that normalization can soften perceived risk.

Yet increasing familiarity did not eliminate wearer-bystander divergence. The expectation-willingness gap remained significant even at the "very familiar" level. Wearers showed a sharp drop in concern, whereas bystanders' decline was gradual, suggesting that deeper understanding does not guarantee convergence but instead reveals enduring asymmetry between roles.

A notable reversal emerged in evaluations of LED indicator sufficiency. For users with low familiarity, "the light is on" signifies transparency and safety, with acceptance peaking at the "very familiar" level. However, current/former users recognize that LEDs are visible yet socially ineffective [3, 121]. This *familiarity paradox* [58] suggests that as users gain deeper understanding of camera-glasses operation, familiarity no longer promotes acceptance but instead reveals the device's covert potential. This effect may be particularly salient for camera glasses, where capture is inherently less visible than in traditional cameras or HMDs [40].

Interestingly, no comparable fluctuation appeared in information transparency or protection demands. One explanation is "privacy resignation": as familiarity increases, bystanders become accustomed to potential risks and pragmatically tolerate data vulnerability while feeling powerless to resist [16, 32, 76]. Alternatively, expectations for transparency and protection may operate at a broader social level rather than being device-specific, producing stable ratings despite continued critical awareness [33, 86]. Future longitudinal work could examine how familiarity interacts with psychological adaptation and regulatory expectations over time.

6.3 Scaling Privacy Negotiation to Complex Settings

While our studies focused on dyadic interactions between a wearer and a bystander, real-world public spaces often involve dynamic, multi-party environments where traditional PETs become impractical due to interaction time and attentional costs [19, 113]. Excessive notifications may intensify usability tensions as audiences grow.

The four trade-offs identified in Study 2 become more pronounced in multi-party settings. The visibility-disruption tension grows as collective awareness requires signals that quickly exceed social comfort. The empowerment-burden tension scales with group size, making multi-party consent unmanageable. The protection-agency tension persists because automated controls cannot eliminate the need for user autonomy. The accountability-exposure tension intensifies as responsibility extends across more actors. These amplified pressures indicate that multi-party privacy negotiation is not simply a scaled-up dyadic problem but a fundamentally different design space.

Building on this logic, adaptive privacy protocols could address these trade-offs by adjusting signals to reduce visibility-disruption tension, simplifying how bystanders express preferences to ease empowerment-burden tensions, and using context-aware automation that preserves user agency. Multi-modal cues may help clarify accountability without creating additional exposure [3, 121]. Such approaches frame privacy not as individual negotiation but as an in-situ, collective process [61].

6.4 Multi-Stakeholder Perspectives and Cultural Considerations

Incorporating a multi-stakeholder perspective revealed that privacy expectations are role-dependent and context-sensitive [29, 90]. Unlike prior work that mainly documents risks or evaluates isolated mechanisms [3, 74], our paired design directly captured experiences and demands from both groups within shared scenarios. This enabled systematic examination of how contextual features shape privacy judgments and helped identify key trade-offs in PET design [23, 25, 131]. In dynamic environments where individuals may shift roles constantly [16], understanding both perspectives provides a foundation for developing protection systems that respond to changing social configurations.

Cultural background further shapes these dynamics [41, 67, 109]. Our Chinese participants, drawn from the world's largest camera glasses market [135, 136], showed high familiarity with domestic brands (87–89% knew Xiaomi) compared to international products (Ray-Ban Meta: 27–44%; Google Glass: 30–32%), partially grounding their evaluations in locally dominant products. Furthermore, people in collectivist cultures may treat privacy more as a social matter, placing greater emphasis on interactional risks than individuals in more individualist contexts [67]. Our sample shows this pattern: dense social networks (74% knew users, 25% knew 3+ users) coexist with strong control expectations (M = 5.99), indicating privacy boundaries shaped through social relationships rather than individual autonomy alone.

These findings suggest that privacy should be understood as a culturally situated negotiation rather than a universal preference. Complementing this work with studies from other societies can help understand how cultural norms [16, 53] influence privacy needs in shared environments. Cultural variation also intersects with identities such as age and ability [5, 106, 141], requiring careful consideration when generalizing findings across contexts.

7 Limitations and Future Work

Several methodological limitations constrain the generalizability of our findings. Our exclusive focus on Chinese participants limits cross-cultural applicability. China's distinct privacy culture, rapid smart glasses adoption, and regulatory environment may produce patterns that do not generalize to Western contexts where privacy expectations differ substantially [81]. The timing of data collection during China's smart glasses market expansion may capture attitudes specific to early adoption phases rather than mature market dynamics.

Study 1's reliance on vignette-based scenarios, while enabling systematic manipulation, cannot capture the emotional intensity and social complexity of actual privacy violations [29]. Self-reported measures introduce potential social desirability effects [38] and privacy paradox concerns [59], though we attempted mitigation through indirect questioning, randomized scenario presentation, and inclusion of both attitudinal and behavioral intention measures. Additionally, our abbreviated baseline attitude scales (2 items each) showed modest internal consistency, particularly for Information Sharing Intention ($\alpha = 0.48$). While convergent validity analyses supported their use as descriptive measures, future research employing baseline attitudes as primary variables should use longer, fully validated scales such as the VOPP [44] or complete IUIPC instruments [73].

Study 2's paired interviews may have encouraged consensus-seeking, and scenario-based PET evaluation cannot replicate real-world implementation constraints. Both samples skewed toward younger, educated, technology-literate participants, potentially underrepresenting broader attitudes. Systematic research on excluded groups, including elderly individuals, children, and people with disabilities, is essential for equitable protection. Importantly, our studies capture stated preferences rather than behavioral evidence. While we provide diagnostic value by quantifying gaps and identifying trade-offs, validating whether these preferences predict real-world behavior requires longitudinal field deployments.

Looking forward, comparative studies across Western and Eastern contexts are essential for developing globally applicable privacy frameworks. Technical research priorities include developing lightweight context recognition systems that identify environmental characteristics without surveillance [104, 138], privacy-preserving negotiation protocols for rapid, anonymous preference expression in ephemeral encounters [10], and aesthetic-preserving privacy filters that protect bystanders without destroying creative intent [26, 82]. Only through such comprehensive approaches can we enable the benefits of wearable cameras while preserving the privacy foundations essential for social trust.

8 Conclusion

This investigation provides a systematic multi-stakeholder evaluation of privacy mechanisms for camera glasses. Through surveys (N=525) and paired interviews (N=20) evaluating 12 PETs, we identified persistent expectation-willingness gaps stemming from four fundamental trade-offs: visibility versus disruption, empowerment versus burden, protection versus agency, and accountability versus exposure.

Context emerged as the primary determinant of privacy acceptability, extending contextual integrity theory to questions of whether sensing should occur. Our context-adaptive pathways progress from minimal-friction visibility in public spaces through structured negotiation in semi-public environments to automatic protection in sensitive contexts. These findings challenge assumptions that better technical mechanisms alone can reconcile privacy conflicts, pointing toward privacy as collectively determined and structurally enforced through coordinated sociotechnical systems.

Acknowledgments

This work is supported by the Natural Science Foundation of China (NSFC) under Grant No. 62472243.

References

[1] Melvin Abraham, Mohamed Khamis, and Mark McGill. 2024. Don't Record My Private pARts: Understanding The Role of Sensitive Contexts and Privacy Perceptions in Influencing Attitudes Towards Everyday Augmented Reality

Sensor Usage. In *2024 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE, 749–758.

[2] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th annual international conference on mobile systems, applications, and services*. 235–248.

[3] 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.

[4] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a limit? privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018), 1–27.

[5] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. 2020. " I am uncomfortable sharing what I can't see": Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications. In *29th USENIX Security Symposium (USENIX Security 20)*. 1929–1948.

[6] Jad Al Aaraj and Athina Markopoulou. 2025. BystandARIA: Enabling AR Bystander Privacy using LEDs. In *Proceedings of the Twenty-sixth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*. 444–449.

[7] Ali Al-Musawi, Erik Yang, Katja Bley, Devinder Thapa, and Ilias O Pappas. 2021. The role of citizens' familiarity, privacy concerns, and trust on adoption of smart services. In *Norsk IKT-konferanse for forskning og utdanning*.

[8] Wael Albayaydh and Ivan Flechais. 2023. Examining power dynamics and user privacy in smart technology use among jordanian households. In *32nd USENIX Security Symposium (USENIX Security 23)*. 4643–4659.

[9] 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.

[10] Ahmed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T Parker, Benjamin Gilbert, and Chuan Yue. 2023. Exploring the negotiation behaviors of owners and bystanders over data practices of smart home devices. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–27.

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

[12] Irwin Altman. 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of social issues* 33, 3 (1977), 66–84.

[13] Ashwin Ashok, Viet Nguyen, Marco Gruteser, Narayan Mandayam, Wenjia Yuan, and Kristin Dana. 2014. Do not share! Invisible light beacons for signaling preferences to privacy-respecting cameras. In *Proceedings of the 1st ACM MobiCom workshop on Visible light communication systems*. 39–44.

[14] Mukhtaj S Barhm, Nidal Qwasmi, Faisal Z Qureshi, and Khalil El-Khatib. 2011. Negotiating privacy preferences in video surveillance systems. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*. Springer, 511–521.

[15] Lemi Baruh and Zeynep Cemalcılar. 2014. It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences* 70 (2014), 165–170.

[16] Divyanshu Bhardwaj, Alexander Ponticello, Shreya Tomar, Adrian Dabrowski, and Katharina Krombholz. 2024. In Focus, Out of Privacy: The Wearer's Perspective on the Privacy Dilemma of Camera Glasses. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–18.

[17] Taryn Bipat, Maarten Willem Bos, Rajan Vaish, and Andrés Monroy-Hernández. 2019. Analyzing the use of camera glasses in the wild. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–8.

[18] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI research: Going behind the scenes*. Morgan & Claypool Publishers.

[19] Cheng Bo, Guobin Shen, Jie Liu, Xiang-Yang Li, YongGuang Zhang, and Feng Zhao. 2014. Privacy. tag: Privacy concern expressed and respected. In *Proceedings of the 12th ACM conference on embedded network sensor systems*. 163–176.

[20] Syed Ibrahim Mustafa Shah Bukhari, Maha Sajid, Bo Ji, and Brendan David-John. 2025. Rethinking Privacy Indicators in Extended Reality: Multimodal Design for Situationally Impaired Bystanders. *arXiv preprint arXiv:2508.07057* (2025).

[21] Jennie Carroll, Steve Howard, Jane Murphy, and John Peck. 2002. 'No'to a free mobile: when adoption is not enough. (2002).

[22] Wan-Jung Chang, Liang-Bi Chen, Chia-Hao Hsu, Jheng-Hao Chen, Tzu-Chin Yang, and Cheng-Pei Lin. 2020. MedGlasses: A wearable smart-glasses-based drug pill recognition system using deep learning for visually impaired chronic patients. *IEEE Access* 8 (2020), 17013–17024.

[23] Ji Won Chung, Xiyu Jenny Fu, Zachary Deocadiz-Smith, Malte F Jung, and Jeff Huang. 2023. Negotiating dyadic interactions through the lens of augmented reality glasses. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*. 493–508.

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

[25] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y Charlie Hu, and Bo Ji. 2023. Securing bystander privacy in mixed reality while protecting the user experience. *IEEE Security & Privacy* 22, 1 (2023), 33–42.

[26] Ana Cassia Cruz, Rogério Luís de C Costa, Leonel Santos, Carlos Rabadão, Anabela Marto, and Alexandrino Gonçalves. 2025. Assessing User Perceptions and Preferences on Applying Obfuscation Techniques for Privacy Protection in Augmented Reality. *Future Internet* 17, 2 (2025), 55.

[27] Brendan David-John, Bo Ji, and Evan Selinger. 2024. Understanding the long-term impact and perceptions of privacy-enhancing technologies for bystander obscuration in AR. In *2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*. IEEE, 23–25.

[28] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–37.

[29] 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.

[30] 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.

[31] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D Abowd, and Sauvik Das. 2021. Smart webcam cover: Exploring the design of an intelligent webcam cover to improve usability and trust. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (2021), 1–21.

[32] Nora A Draper. 2017. From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates. *Policy & Internet* 9, 2 (2017), 232–251.

[33] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 5257–5261.

[34] Serge Egelman and Eyal Peer. 2015. Predicting privacy and security attitudes. *ACM SIGCAS computers and society* 45, 1 (2015), 22–28.

[35] Michael Eisenberg and Carol Barry. 1988. Order effects: A study of the possible influence of presentation order on user judgments of document relevance. *Journal of the American Society for Information Science* 39, 5 (1988), 293–300.

[36] Lisa A Elkin, Matthew Kay, James J Higgins, and Jacob O Wobbrock. 2021. An aligned rank transform procedure for multifactor contrast tests. In *The 34th annual ACM symposium on user interface software and technology*. 754–768.

[37] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. 2022. Transparency for Bystanders in IoT regarding audiovisual Recordings. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 649–654.

[38] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of consumer research* 20, 2 (1993), 303–315.

[39] Joshua Fogel and Elham Nehmad. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior* 25, 1 (2009), 153–160.

[40] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative privacy concerns about ar glasses data collection. *Proceedings on Privacy Enhancing Technologies* (2023).

[41] Reza Ghaiumy Anaraky, Yao Li, and Bart Knijnenburg. 2021. Difficulties of measuring culture in privacy studies. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–26.

[42] Sindhu Reddy Kalathur Gopal, Diksha Shukla, James David Wheelock, and Nitesh Saxena. 2023. Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all!. In *32nd USENIX security symposium (USENIX Security 23)*. 859–876.

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

[44] Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. A psychometric scale to measure individuals' value of other people's privacy (VOPP). In *Proceedings of the 2023 chi conference on human factors in computing systems*. 1–14.

[45] Benjamin Henne, Christian Szongott, and Matthew Smith. 2013. SnapMe if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. 95–106.

[46] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing*. 571–582.

[47] Mina Huh, Zihui Xue, Ujjaini Das, Kumar Ashutosh, Kristen Grauman, and Amy Pavel. 2025. Vid2Coach: Transforming How-To Videos into Task Assistants. In *Proceedings of the 38th Annual ACM Symposium on User Interface Software and Technology*. 1–24.

[48] Apple Inc. 2024. What EyeSight shows on Apple Vision Pro. https://support.apple.com/en-us/120481. [Accessed 04-09-2025].

[49] Snap Inc. 2025. LED Messages — support.spectacles.com. https://support.spectacles.com/hc/en-us/articles/360033763171-LED-Messages. [Accessed 04-09-2025].

[50] Muhammad Zahid Iqbal and Abraham G Campbell. 2023. Adopting smart glasses responsibly: potential benefits, ethical, and privacy concerns with Ray-Ban stories. *AI and Ethics* 3, 1 (2023), 325–327.

[51] Alberto Escalada Jimenez, Adrian Dabrowski, Noburu Sonehara, Juan M Montero Martinez, and Isao Echizen. 2014. Tag detection for preventing unauthorized face image processing. In *International Workshop on Digital Watermarking*. Springer, 513–524.

[52] Adam N Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. 2010. Privacy, trust, and self-disclosure online. *Human–Computer Interaction* 25, 1 (2010), 1–24.

[53] Se Jung Kim, Yoon Esther Lee, and T Makana Chock. 2025. Cultural Differences in the Use of Augmented Reality Smart Glasses (ARSGs) Between the US and South Korea: Privacy Concerns and the Technology Acceptance Model. *Applied Sciences* 15, 13 (2025), 7430.

[54] Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie Kaufman. 2023. Erebus: Access control for augmented reality systems. In *32nd USENIX Security Symposium (USENIX Security 23)*. 929–946.

[55] Marion Koelle, Swamy Ananthanarayan, Simon Czupalla, Wilko Heuten, and Susanne Boll. 2018. Your smart glasses' camera bothers me! exploring opt-in and opt-out gestures for privacy mediation. In *Proceedings of the 10th Nordic Conference on Human-Computer Interaction*. 473–481.

[56] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't look at me that way! Understanding user attitudes towards data glasses usage. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*. 362–372.

[57] Marion Koelle, Torben Wallbaum, Wilko Heuten, and Susanne Boll. 2019. Evaluating a Wearable Camera's Social Acceptability In-the-Wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[58] 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.

[59] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[60] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2015. Ok glass, leave me alone: towards a systematization of privacy enhancing technologies for wearable computing. In *International Conference on Financial Cryptography and Data Security*. Springer, 274–280.

[61] Olya Kudina and Peter-Paul Verbeek. 2019. Ethics from within: Google Glass, the Collingridge dilemma, and the mediated value of privacy. *Science, Technology, & Human Values* 44, 2 (2019), 291–314.

[62] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann.

[63] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 392–408.

[64] EunWon Lee and GyeongAe Seomun. 2021. Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *International journal of environmental research and public health* 18, 4 (2021), 2084.

[65] Ang Li, Qinghua Li, and Wei Gao. 2016. Privacycamera: Cooperative privacy-aware photographing with mobile phones. In *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 1–9.

[66] Fenghua Li, Zhe Sun, Ang Li, Ben Niu, Hui Li, and Guohong Cao. 2019. Hideme: Privacy-preserving photo sharing on social networks. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 154–162.

[67] Yao Li, Eugenia Ha Rim Rho, and Alfred Kobsa. 2022. Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology* 41, 3 (2022), 655–677.

[68] Si Liao, Hanwei He, Huangxun Chen, and Zhice Yang. 2025. Bystander Privacy in Video Sharing Era: Automated Consent Compliance through Platform Censorship. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–16.

[69] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2019. Understanding the role of privacy and trust in intelligent personal assistant adoption. In *International conference on information*. Springer, 102–113.

[70] Natasha Lomas. 2021. Facebook warned over 'very small' indicator LED on smart glasses, as EU DPAs flag privacy concerns. https://techcrunch.com/2021/09/20/facebook-warned-over-very-small-indicator-led-on-smart-glasses-as-eu-dpas-flag-privacy-concerns. [Accessed 16-08-2025].

[71] Chen-Chung Ma, Kuang-Ming Kuo, and Judith W Alexander. 2015. A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC medical informatics and decision making* 16, 1 (2015), 13.

[72] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology* 19, 5 (1983), 469–479.

[73] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[74] Shady Mansour, Pascal Knierim, Joseph O'Hagan, Florian Alt, and Florian Mathis. 2023. Bans: Evaluation of bystander awareness notification systems for productivity in vr. In *Network and Distributed Systems Security (NDSS) Symposium*, Vol. 2.

[75] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. 83–95.

[76] 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.

[77] Philipp Mayring. 2014. Qualitative content analysis: theoretical foundation, basic procedures and software solution. (2014).

[78] Terence V McCann and Eileen Clark. 2003. Grounded theory in nursing research: Part 1–Methodology. (2003).

[79] Daniel McDuff and Christophe Hurter. 2018. Inphysible: Camouflage against video-based physiological measurement. In *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 5784–5789.

[80] Franziska Meirose, Sven Schultze, Sebastian Kuehlewind, Marion Koelle, Larbi Abdenebaoui, and Susanne Boll. 2018. Towards Respectful Smart Glasses through Conversation Detection.. In *MuC*.

[81] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European journal of information systems* 23, 2 (2014), 103–125.

[82] Tamara Mujirishvili, Anton Fedosov, Kooshan Hashemifard, Pau Climent-Pérez, and Francisco Florez-Revuelta. 2024. "I Don't Want to Become a Number": Examining Different Stakeholder Perspectives on a Video-Based Monitoring System for Senior Care with Inherent Privacy Protection (by Design).. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–19.

[83] David H Nguyen, Aurora Bedford, Alexander Gerard Bretana, and Gillian R Hayes. 2011. Situating the concern for information privacy through an empirical study of responses to video recording. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3207–3216.

[84] David H Nguyen, Gabriela Marcu, Gillian R Hayes, Khai N Truong, James Scott, Marc Langheinrich, and Christof Roduner. 2009. Encountering SenseCam: personal recording technologies in everyday life. In *Proceedings of the 11th international conference on Ubiquitous computing*. 165–174.

[85] Molly Jane Nicholas, Brian A Smith, and Rajan Vaish. 2022. Friendscope: Exploring In-the-Moment Experience Sharing on Camera Glasses via a Shared Camera. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 1–25.

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

[87] Yuqi Niu, Nicole Meng-Schneider, Weidong Qiu, and Nadin Kokciyan. 2025. "I am not the primary focus"-Understanding the Perspectives of Bystanders in Photos Shared Online. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–23.

[88] Yuqi Niu, Weidong Qiu, Peng Tang, Lifan Wang, Shuo Chen, Shujun Li, Nadin Kökciyan, and Ben Niu. 2025. Everyone's Privacy Matters! An Analysis of Privacy Leakage from Real-World Facial Images on Twitter and Associated User Behaviors. *Proceedings of the ACM on Human-Computer Interaction* 9, 2 (2025), 1–38.

[89] Joseph O'Hagan, Jan Gugenheimer, Jolie Bonner, Florian Mathis, and Mark McGill. 2023. Augmenting people, places & media: The societal harms posed

by everyday augmented reality, and the case for perceptual human rights. In *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia*. 225–235.

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

[91] Judith S Olson, Jonathan Grudin, and Eric Horvitz. 2005. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*. 1985–1988.

[92] Matthew J Page, Joanne E McKenzie, Patrick M Bossuyt, Isabelle Boutron, Tammy C Hoffmann, Cynthia D Mulrow, Larissa Shamseer, Jennifer M Tetzlaff, Elie A Akl, Sue E Brennan, et al. 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj* 372 (2021).

[93] Shwetak N Patel, Jay W Summet, and Khai N Truong. 2009. Blindspot: Creating capture-resistant spaces. In *Protecting Privacy in Video Surveillance*. Springer, 185–201.

[94] Alfredo J Perez, Sherali Zeadally, and Scott Griffith. 2017. Bystanders' privacy. *IT Professional* 19, 3 (2017), 61–65.

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

[96] Alfredo J Perez, Sherali Zeadally, Luis Y Matos Garcia, Jaouad A Mouloud, and Scott Griffith. 2018. FacePET: Enhancing bystanders' facial privacy with smart wearables/internet of things. *Electronics* 7, 12 (2018), 379.

[97] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. 2011. Notisense: An urban sensing notification system to improve bystander privacy. In *Proceedings of the 2nd International Workshop on Sensing Applications on Mobile Phones (PhoneSense), Seattle, WA, USA*. 12–15.

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

[99] Rebecca S Portnoff, Linda N Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's watching me? assessing the effectiveness of webcam indicator lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1649–1658.

[100] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. Priview–exploring visualisations to support users' privacy awareness. In *Proceedings of the 2021 chi conference on human factors in computing systems*. 1–18.

[101] Jason Procyk, Carman Neustaedter, Carolyn Pang, Anthony Tang, and Tejinder K Judge. 2014. Exploring video streaming in public settings: shared geocaching over distance using mobile video chat. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2163–2172.

[102] 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.

[103] Shwetha Rajaram, Jiasi Chen, and Michael Nebeling. 2025. Privacy Equilibrium: Balancing Privacy Needs in Dynamic Multi-User Augmented Reality Scenarios. In *Proceedings of the 38th Annual ACM Symposium on User Interface Software and Technology*. 1–24.

[104] Shwetha Rajaram, Macarena Peralta, Janet G Johnson, and Michael Nebeling. 2025. Exploring the Design Space of Privacy-Driven Adaptation Techniques for Future Augmented Reality Interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–19.

[105] Shwetha Rajaram, Franziska Roesner, and Michael Nebeling. 2023. Reframe: An augmented reality storyboarding tool for character-driven analysis of security & privacy concerns. In *Proceedings of the 36th annual ACM symposium on user interface software and technology*. 1–15.

[106] Ashwini Rao and Juergen Pfeffer. 2020. Types of privacy expectations. *Frontiers in big Data* 3 (2020), 7.

[107] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. " You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 143–157.

[108] Reuters. 2003. Korea: Beeping Prevents Peeping — wired.com. https://www.wired.com/2003/11/korea-beeping-prevents-peeping. [Accessed 04-09-2025].

[109] John M Roberts and Thomas Gregor. 2017. Privacy: A cultural view. In *Privacy and Personality*. Routledge, 199–225.

[110] Franziska Roesner, David Molnar, Alexander Moshchuk, Tadayoshi Kohno, and Helen J Wang. 2014. World-driven access control for continuous sensing. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. 1169–1181.

[111] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[112] Jiayu Shu, Rui Zheng, and Pan Hui. 2016. Cardea: Context-aware visual privacy protection from pervasive cameras. *arXiv preprint arXiv:1610.00889* (2016).

[113] Jiayu Shu, Rui Zheng, and Pan Hui. 2017. Your privacy is in your hand: Interactive visual privacy control with tags and gestures. In *International Conference on Communication Systems and Networks*. Springer, 24–43.

[114] Jiayu Shu, Rui Zheng, and Pan Hui. 2018. Cardea: Context-aware visual privacy protection for photo taking and sharing. In *Proceedings of the 9th ACM Multimedia Systems Conference*. 304–315.

[115] 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.

[116] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. 2019. Privaceye: privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features. In *Proceedings of the 11th ACM symposium on eye tracking research & applications*. 1–10.

[117] Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 1553–1562.

[118] Yuanyi Sun, Shiqing Chen, Sencun Zhu, and Yu Chen. 2020. iRyP: a purely edge-based visual privacy-respecting system for mobile cameras. In *Proceedings of the 13th ACM conference on security and privacy in wireless and mobile networks*. 195–206.

[119] Robert Templeman, Mohammed Korayem, David J Crandall, and Apu Kapadia. 2014. PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces.. In *NDSS*, Vol. 14. 23–26.

[120] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–13.

[121] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–13.

[122] James Thomas and Angela Harden. 2008. Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC medical research methodology* 8, 1 (2008), 45.

[123] Tram Thi Minh Tran, Shane Brown, Oliver Weidlich, Soojeong Yoo, and Callum Parker. 2025. Wearable AR in Everyday Contexts: Insights from a Digital Ethnography of YouTube Videos. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–18.

[124] Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Samuel T King, and Zubair Shafiq. 2024. Aragorn: A privacy-enhancing system for mobile cameras. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 7, 4 (2024), 1–31.

[125] M Vimalkumar, Sujeet Kumar Sharma, Jang Bahadur Singh, and Yogesh K Dwivedi. 2021. 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior* 120 (2021), 106763.

[126] V.Magazine. 2025. Ray-Ban Meta Smart Glasses Global Sales Surpass 2 Million Units! The Next Anticipated Target Could Be Prada Meta! https://www.vmagazine.hk/2025/07/29/ray-ban-meta-smart-glasses-global-sales-surpass-2-million-units-the-next-anticipated-target-could-be-prada-meta/. [Accessed 16-08-2025].

[127] Tom Wheeler. 2021. Seeing past the cool: Facebook's new smart glasses | Brooking. https://www.brookings.edu/articles/seeing-past-the-cool-facebooks-new-smart-glasses/. [Accessed 16-08-2025].

[128] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I Hong, and John Zimmerman. 2011. Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th international conference on Ubiquitous computing*. 197–206.

[129] Julie R Williamson, Joseph O'Hagan, John Alexis Guerra-Gomez, John H Williamson, Pablo Cesar, and David A Shamma. 2022. Digital proxemics: Designing social and collaborative interaction in virtual environments. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–12.

[130] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S Feger. 2022. Automating contextual privacy policies: Design and evaluation of a production tool for digital consumer privacy awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–18.

[131] Maximiliane Windl, Petra Zsofia Laboda, and Sven Mayer. 2025. Designing Effective Consent Mechanisms for Spontaneous Interactions in Augmented Reality. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–18.

[132] Maximiliane Windl, Verena Winterhalter, Albrecht Schmidt, and Sven Mayer. 2023. Understanding and mitigating technology-facilitated privacy violations in the physical world. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[133] Jacob O Wobbrock, Leah Findlater, Darren Gergle, and James J Higgins. 2011. The aligned rank transform for nonparametric factorial analyses using only anova procedures. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 143–146.

[134] Katrin Wolf, Karola Marky, and Markus Funk. 2018. We should start thinking about privacy implications of sonic input in everyday augmented reality!. In *Mensch und Computer 2018-Workshopband*. Gesellschaft für Informatik eV, 10–18420.

[135] VRAR World. 2025. IDC Forecasts 107% Year-on-Year Growth for Chinas Smart Glasses Shipments, Projected to Reach 2.75 Million Units in 2025. https://www.xrom.in/post/idc-forecasts-107-year-on-year-growth-for-chinas-smart-glasses-shipments-projected-to-reach-2-75-mi. [Accessed 19-08-2025].

[136] VRAR World. 2025. Xiaomi Raises AI Smart Glasses Sales Target to 500,000 Units. https://www.xrom.in/post/xiaomi-raises-ai-smart-glasses-sales-target-to-500-000-units. [Accessed 19-08-2025].

[137] Yanlai Wu, Xinning Gui, Yuhan Luo, and Yao Li. 2024. Designing the informing process with streamers and bystanders in live streaming. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 315–332.

[138] Yaqing Yang, Tony W Li, and Haojian Jin. 2024. On the Feasibility of Predicting Users' Privacy Concerns using Contextual Labels and Personal Preferences. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–20.

[139] Lan Zhang, Xiang-Yang Li, Kebin Liu, Cihang Liu, Xuan Ding, and Yunhao Liu. 2018. Cloak of invisibility: Privacy-friendly photo capturing and sharing system. *IEEE Transactions on Mobile Computing* 18, 11 (2018), 2488–2501.

[140] Zhan Zhang, Enze Bai, Yincao Xu, Kathleen Adelgais, and Mustafa Ozkaynak. 2025. Can you see what I see? Examining the Impact of Smart Glasses on Communication Dynamics in Distributed Emergency Medical Teams. *Proceedings of the ACM on Human-Computer Interaction* 9, 7 (2025), 1–34.

[141] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. 2023. {"If} sighted people know, I should be able to {know:"} Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology. In *32nd USENIX Security Symposium (USENIX Security 23)*. 4661–4678.

[142] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring privacy to the table: Interactive negotiation for privacy settings of shared sensing devices. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–22.

A Study 1 Survey Instruments

This appendix presents the complete survey instruments used in Study 1. Both surveys were administered in Chinese and translated to English for presentation. Items were rated on 7-point Likert scales unless otherwise specified.

A.1 Baseline Attitude Scales

A.1.1 Bystander Privacy Concerns Scale. Adapted from the Internet Users' Information Privacy Concerns (IUIPC) scale [73] to assess bystanders' baseline privacy attitudes toward smart glasses recording. Participants rated their agreement from 1 (Strongly Disagree) to 7 (Strongly Agree).

A.1.2 Wearer Privacy Responsibility Scale. Developed based on Protection Motivation Theory [72, 111] to assess wearers' baseline attitudes toward protecting bystanders' privacy. Participants rated their agreement from 1 (Strongly Disagree) to 7 (Strongly Agree).

A.2 Contextual Scenario Descriptions

Participants evaluated six scenarios systematically varying across physical setting (public, semi-public, private/sensitive) and social relationship (acquaintance, stranger). Scenarios were presented in randomized order. For bystanders, scenarios described encountering others using smart glasses; for wearers, scenarios described using smart glasses themselves.

A.3 Contextual Measurement Items

For each scenario, participants responded to the following items. Bystanders rated their expectations/needs; wearers rated their willingness to provide.

A.3.1 Privacy Concern and Recording Reasonability.

- **Bystanders:** "In this scenario, to what extent would you be concerned about your privacy?" (1 = Not Concerned at All, 7 = Highly Concerned)
- **Wearers:** "In this scenario, how reasonable do you think it is to use smart glasses for recording?" (1 = Completely Unreasonable, 7 = Highly Reasonable)
- **Wearers:** "In this scenario, to what extent would you be concerned about affecting the privacy of those being recorded?" (1 = Not Concerned at All, 7 = Highly Concerned)

A.3.2 Information Transparency Dimensions. Bystanders rated their need for information (1 = Do Not Need at All, 7 = Strongly Need); wearers rated their willingness to disclose (1 = Very Unwilling, 7 = Very Willing).

A.3.3 Protective Measure Dimensions. Bystanders rated their expectations (1 = Do Not Need at All, 7 = Strongly Need); wearers rated their willingness to adopt (1 = Very Unwilling, 7 = Very Willing).

A.3.4 Behavioral Response (Bystanders Only). Bystanders selected anticipated responses if they discovered being recorded (multiple selections allowed):

- Take no action
- Try to avoid the camera
- Use gestures or actions to express discomfort
- Directly ask the person to stop recording
- Request deletion of data containing them
- File a complaint or report to authorities

A.4 LED Indicator Evaluation

Both groups evaluated current LED notification mechanisms.

Adequacy Assessment: "Most current smart glasses use LED indicators to signal recording. Do you think this method adequately protects [bystanders' privacy / the privacy of those around you]?" (1 = Very Insufficient, 5 = Very Sufficient)

Reasons for Insufficiency (multiple selections allowed):

- Light too small and easily overlooked by people around
- Invisible in bright environments
- Bystander unfamiliar with LED meaning cannot recognize it
- Can be blocked or modified by users
- Cannot distinguish between photo, video, or livestream modes
- Recording range and resolution unclear
- Other: ____________________

Preferred Notification Methods (multiple selections allowed):

- No additional methods needed
- Audio notifications (shutter sound or voice prompt)
- Push notifications to nearby smartphones
- Verbal notification from recorder
- More visible visual indicators
- Other: ____________________

Table 4: Bystander Privacy Concerns Scale Items

Dimension	Item
Awareness	AW1: I pay attention to whether I am being photographed or recognized by smart glasses without being informed. AW2: I pay attention to whether I am being photographed or recognized by smart glasses without my consent.
Control	CT1: I should have the right to decide whether to be photographed by smart glasses and how my image is used. CT2: If I notice I might be photographed by smart glasses, I would take action to avoid entering the frame or decline recording.
Collection	CL1: When I notice I might be photographed or recognized by smart glasses, I pay attention to potential implications for my personal privacy. CL2: I pay attention to whether my image captured by smart glasses might be used or shared by others.

Table 5: Wearer Privacy Responsibility Scale Items

Dimension	Item
Perceived Responsibility	PR1: I have a responsibility to protect the privacy of people around me when using smart glasses. PR2: When using smart glasses in public places, I consider whether my recording behavior might cause dissatisfaction or other consequences for others.
Information Sharing Intention	IS1: When using smart glasses' recording or recognition functions, I prefer to inform those around me. IS2: If people around me want to understand the recording situation, I am willing to inform them of my recording purpose and data usage.
Privacy Protection Intention	PP1: Before using smart glasses for recording or recognition, I should obtain consent from relevant people. PP2: If people around me express concerns or objections, I am willing to stop or adjust my recording behavior.

Table 6: Contextual Scenario Design

Scenario	Setting	Relationship	Context Description
Street	Public	Acquaintance	Recording travel scenery with companions
Mall	Public	Stranger	Recording shopping vlog in crowded space
Meeting	Semi-public	Acquaintance	Recording meeting for personal minutes
Hospital	Semi-public	Stranger	Recording navigation and procedures
Private Party	Private	Acquaintance	Recording social gathering at home
Gym	Sensitive	Stranger	Recording workout with others present

Motivators for Privacy-Protective Practices (multiple selections allowed):

- Technical convenience and ease of use
- Being in sensitive locations
- Social pressure (avoiding dissatisfaction or conflict)
- Respect and moral responsibility
- Social incentives (receiving praise or recognition)
- Legal and regulatory requirements
- Other: ____________________

B Study 1 Supplementary Materials

B.1 Participant Demographics and Baseline Characteristics

Table 9 presents the demographic characteristics and baseline attitudes of participants in Study 1.

Table 7: Information Transparency Items

Dimension	Item
Purpose	Purpose and intended use of recording
Sharing	Whether data will be uploaded, shared, or made public
AI Use	Whether data will be analyzed by AI or algorithms
Retention	Data storage method and retention duration
Content	Specific content of the recording

Table 8: Protective Measure Items

Measure	Item
Proactive Notification	Proactively notify about recording behavior
Privacy Filter	Apply privacy protection (e.g., automatic face blurring)
No Sharing	Ensure recorded data will not be uploaded or shared
Auto Delete	Ensure recorded data will be automatically deleted after a period
Prior Consent	Only record after obtaining consent

B.2 Convergent Validity of Baseline Measures

To assess whether our abbreviated baseline measures behaved in line with theoretical expectations, we examined their correlations with scenario-based measures (Figure 14).

For bystanders, all six baseline items showed positive correlations with scenario-averaged privacy concerns, information needs, and protective measure demands ($r \approx .12–.42$, most $ps < .001$). Participants reporting higher baseline concern also reported stronger scenario-based privacy concerns and requested more extensive protections.

For wearers, the pattern was more pronounced. Baseline items capturing perceived responsibility, privacy protection intention, and information sharing intention correlated positively with scenario-averaged disclosure willingness and willingness to adopt PETs ($r \approx .25–.62$, $ps < .001$). Notably, despite modest internal consistency ($\alpha = 0.48$), Information Sharing Intention items showed substantial correlations with scenario-based disclosure willingness ($r = .42–.59$), supporting their validity as descriptive measures.

These patterns confirm convergent validity: baseline measures relate to scenario-specific outcomes in theoretically expected directions. Given their brevity, we treat these scales as descriptive rather than primary constructs.

Table 9: Participant Demographics and Baseline Characteristics

Characteristic	Bystanders (N=293)	Wearers (N=232)
Gender		
Male	49.2%	59.5%
Female	50.5%	39.2%
Non-binary/Other	0.3%	1.3%
Age		
18–25 years	39.6%	32.3%
26–35 years	53.2%	51.3%
36–45 years	5.1%	14.2%
46+ years	2.0%	2.2%
Smart Glasses Familiarity		
Never heard of	4.8%	0.0%
Heard of but unfamiliar	28.3%	13.8%
Understand basic functions	46.8%	35.3%
Very familiar	15.7%	27.6%
Current/former user	4.4%	23.3%
Acquaintances Using Smart Glasses		
None	25.9%	28.9%
1 person	25.9%	24.1%
2 people	23.2%	18.5%
3+ people	24.9%	28.4%
Brand Awareness		
Xiaomi AI Glasses	87.7%	89.2%
Rayneo V3/X3 Series	49.1%	60.3%
Ray-Ban Meta/Oakley Meta	27.0%	43.5%
Google Glass	29.7%	31.9%
Rokid Glasses	21.8%	34.9%
Baseline Attitudes		
Awareness / Perceived Responsibility	5.76 ± 1.15	5.94 ± 1.19
Control / Information Sharing Intention	5.99 ± 0.93	5.75 ± 1.32
Collection / Privacy Protection Intention	5.53 ± 1.19	5.98 ± 1.14

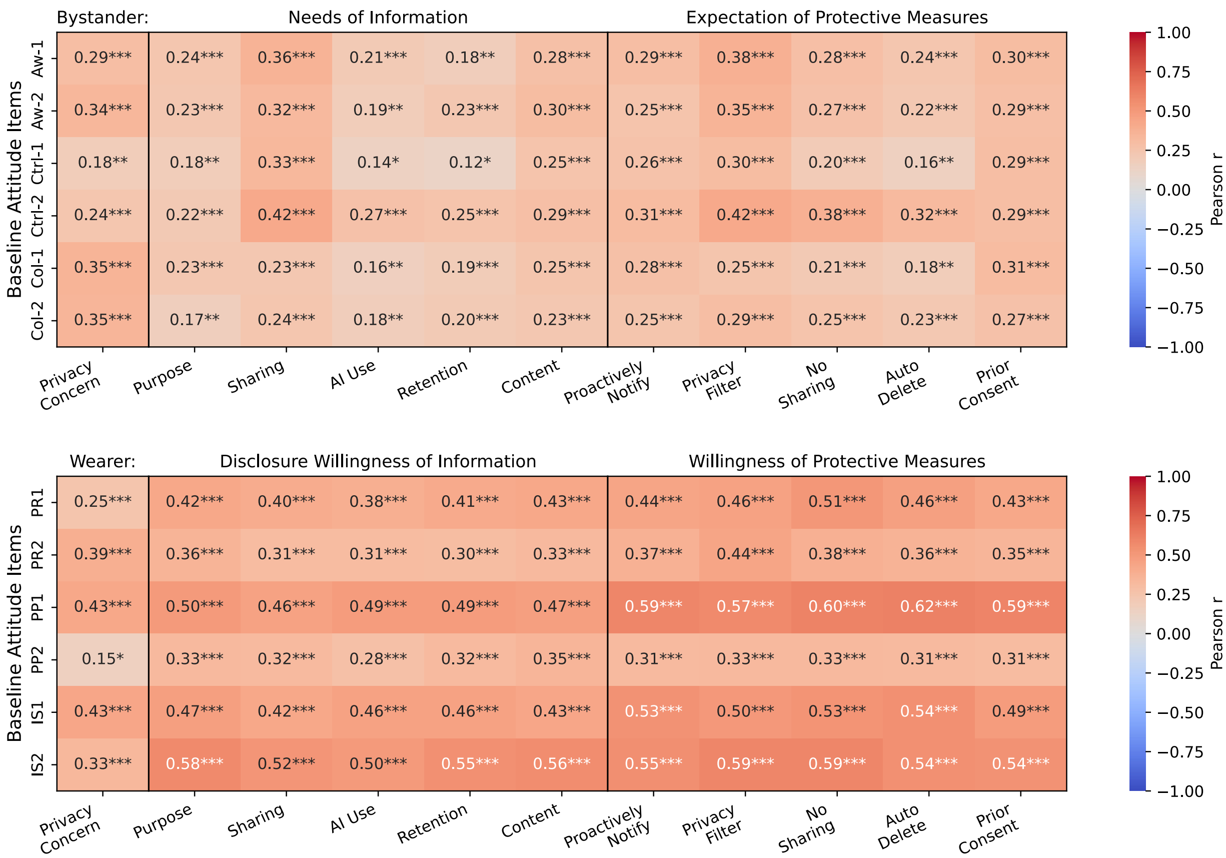

Figure 14: Pearson correlations between baseline attitude items and scenario-averaged measures. Top panel: Bystanders' baseline attitudes (Awareness: Aw-1, Aw-2; Control: Ctrl-1, Ctrl-2; Collection: Col-1, Col-2) correlated with their average ratings of privacy concerns, information needs, and expectations for protective mechanisms across scenarios. Bottom panel: Wearers' baseline items (Perceived Responsibility: PR1, PR2; Privacy Protection Intention: PP1, PP2; Information Sharing Intention: IS1, IS2) correlated with their scenario-averaged disclosure willingness and willingness to adopt protective measures. Cells display Pearson's r; asterisks indicate significance levels (* p < .05, ** p < .01, *** p < .001). Darker shading represents stronger positive correlations.