Privacy Usability Evaluation of IoT Smart Home Companion Application: A Pilot Study of the ABCDE Privacy Framework with an Industrial Multidisciplinary Team

Amparo Coiduras-Sanagustín *, Eduardo Manchado-Pérez, César García-Hernández

Posted Date: 16 March 2026

doi: 10.20944/preprints202603.1128.v1

Keywords: privacy usability; IoT companion applications; heuristic evaluation; Privacy by Design (PbD); smart home; ABCDE Privacy Framework; multidisciplinary teams

 doi:10.20944/preprints202603.1128.v1

Article

Privacy Usability Evaluation of IoT Smart Home Companion Application: A Pilot Study of the ABCDE Privacy Framework with an Industrial Multidisciplinary Team

Amparo Coiduras-Sanagustín [1,2,*], Eduardo Manchado-Pérez [2] and César García-Hernández [2]

[1] School of Architecture and Technology, San Jorge University, Spain
[2] Engineering and Architecture School, University of Zaragoza, Spain
* Correspondence: macoiduras@usj.es

Abstract

Privacy usability in IoT smart home companion applications remains an underexplored domain despite mounting regulatory requirements and accelerating user adoption. Heuristic evaluation offers a scalable pathway to privacy usability assessment, yet validated frameworks for applying such methods are scarce. This study presents the first empirical application of the ABCDE Privacy Framework, a ten-heuristic instrument grounded in Nielsen's usability principles and Privacy by Design, to an IoT companion application developed with a major European home appliance manufacturer. A structured workshop was conducted with a multidisciplinary team of seven participants (five industry professionals and two researchers) following a two-round protocol: a qualitative heuristic discussion phase (Round 1) and an individual scoring phase (Round 2). Data were analysed through MAXQDA. Average heuristic scores ranged from 3.6 (H9: error recovery) to 4.8 (H6: recognition; H10: documentation), with an overall mean of 4.32. Six second-order themes were identified, including Transparency Asymmetry, Centralised but Decontextualised Privacy, and Shared Household Complexity. The ABCDE Privacy Framework is feasible, time-efficient, and analytically productive in real industrial contexts, generating design-relevant insights and enabling cross-role team alignment within a two-hour session. These findings support its potential as a scalable tool for Privacy by Design practice in IoT product development.

Keywords: privacy usability; IoT companion applications; heuristic evaluation; Privacy by Design (PbD); smart home; ABCDE Privacy Framework; multidisciplinary teams

1. Introduction

Connected products have become a defining feature of contemporary domestic and industrial environments. Smart appliances, wearable devices, vehicles, and monitoring systems are no longer standalone objects but nodes in broader digital ecosystems, inseparable from the cloud services, data flows, and companion interfaces that enable their operation (Ashton, 2009; Rose et al., 2015; Redström & Wiltse, 2019). This paradigm, broadly captured under the concept of the Internet of Things (IoT), has opened significant opportunities for product innovation and service development while simultaneously introducing complex challenges around data privacy, user autonomy, and trust (Westin, 1967; Nissenbaum, 2010; Solove, 2006).

Privacy in IoT product development can no longer be treated as a compliance matter to be resolved after design decisions have been made (Langheinrich, 2001; Friedman et al., 2002). It is a core design concern that shapes how interfaces are structured, how data practices are communicated, and how much genuine control users are afforded over their personal information. The mobile and web-based companion applications through which users configure and monitor connected devices

 doi:10.20944/preprints202603.1128.v1

are particularly critical in this regard: the design choices embedded in these interfaces directly determine whether privacy is experienced as legible and controllable, or as opaque and imposed (Lederer et al., 2004; Böhme & Köpsell, 2010). Yet despite growing awareness of this challenge, design and engineering teams working in industrial contexts frequently lack structured, practical methods for evaluating and improving privacy usability as part of their iterative development process (Cranor & Garfinkel, 2005; Distler et al., 2021).

The present study reports the empirical application of the ABCDE Privacy Framework in a real industrial setting. The study was with the team members of a large European home appliance manufacturer. This company is referred to throughout this study as Company X in accordance with the organisation's preference for confidentiality, whose consumer-facing IoT companion application served as the object of assessment. The application enables users to remotely connect, monitor, and control a range of smart household appliances, including dishwashers, washing machines, ovens, and cooktops, via a dedicated smartphone companion app (Rowland et al., 2015). It constitutes a representative example of the privacy-sensitive digital interfaces that the ABCDE Privacy Framework is designed to evaluate (Lederer et al., 2004). Where handling personal registration data, usage analytics, appliance operational data, device-sharing configurations, and multiple categories of privacy-relevant communication happens across varied interface contexts (Nissenbaum, 2010).

The pilot study pursued two interrelated objectives. The first was methodological, to determine whether the ABCDE Privacy Framework could be feasibly and productively done in a real organisational context, with industry professionals working under genuine operational constraints, within a two-hour time-bounded session, and using an online video conferencing platform (Zimmerman et al., 2007). The second was empirical, to generate preliminary substantive findings regarding the privacy usability of the evaluated application, demonstrating both the analytical depth and the design-oriented output that the framework is capable of producing (Iachello & Hong, 2007; Nielsen, 1994).

The first section describes the study context and the industrial partner's digital product, followed by the participant profiles. A dedicated section then describes the preparation phase conducted prior to the main session, and another presents the workshop structure and protocol as realised. The qualitative findings from Round 1 are presented across two sections, the first organised heuristic by heuristic, and the second through systematic thematic coding analysis supported by MAXQDA visualisations (VERBI Software, 2023). The quantitative results follow, including the radar chart produced during the session. The study closes with sections addressing participant feedback, discussion, limitations, and summary.

2. Materials and Methods

The pilot study was conducted with the digital product team of Company X, a major European manufacturer of connected home appliances with a broad international commercial presence. The company is part of one of Europe's largest and most established industrial groups, with decades of experience in consumer appliance manufacturing, a portfolio spanning multiple internationally recognised brands, and operations across more than fifty countries worldwide. Its digital product division represents a significant and strategic investment in the connected home ecosystem (Chesbrough, 2003), reflecting the organisation's commitment to integrating IoT capabilities across its full range of household appliances (Rose et al., 2015). Securing the participation of a team of this scale and institutional weight for an academic pilot study represents a meaningful validation of the research's relevance to real industrial practice.

The company develops and maintains a digital companion application that allows end users to remotely connect, monitor, and operate a wide range of IoT-enabled household appliances, including dishwashers, washing machines, ovens, refrigerators, and cooktops, via a dedicated smartphone interface. At the time of the study, the application was available across multiple European markets and had a significant number of active users.

 doi:10.20944/preprints202603.1128.v1

From a privacy usability perspective, the application constitutes a particularly pertinent object of assessment. It handles multiple categories of personally identifying and behavioural data: registration and account credentials, home location and usage preferences, appliance operational data (including timing patterns and programme choices), and third-party analytics data collected to support service improvement. The onboarding flow requires users to agree to privacy and data collection terms, configure permissions and notification preferences, and establish a user account linked to their physical appliances (Böhme & Köpsell, 2010). These processes involve a series of privacy-relevant decisions communicated through interface elements whose clarity, accessibility, and design quality are precisely what the ABCDE Privacy Framework is designed to evaluate (Lederer et al., 2004; Nielsen, 1994).

2.1. Participants

The organisation's product team was recruited for this pilot study on the basis of several criteria: the direct relevance of their digital product to the IoT privacy domain addressed by the ABCDE Privacy Framework; the multidisciplinary professional composition of the team, which is optimal for the framework's application protocol; their capacity to provide access to a live product for evaluation purposes; and their expressed willingness to engage in a structured research collaboration within a defined time frame. Prior to the workshop session, a series of preparatory meetings were held with the company's Product Manager, in order to present the framework, explain the workshop protocol and its objectives, align expectations regarding the scope and format of the evaluation, and ensure that the necessary organisational and logistical conditions were in place for its successful implementation. In accordance with the organisation's confidentiality requirements, the company name, product name, and all participant identifiers are anonymised throughout this study. Participants are identified by speaker code and professional role.

Seven participants took part in the pilot workshop, representing six distinct professional roles. Five were industry professionals from Company X's digital product team; specifically, their roles included spanning product management, analytics, engineering, and platform operations and two were members of the research team responsible for designing and facilitating the session. This composition was intentional and central to the ABCDE Privacy Framework's design, which is conceived to facilitate structured dialogue across the professional perspectives, such as technical, experiential, analytical, operational, and design-oriented that characteristically coexist in industrial product development contexts. The diversity of these perspectives is considered a methodological asset, as privacy usability encompasses concerns that do not fall neatly within any single functional domain and benefit from cross-role interrogation (Acquisti et al., 2015).

The workshop session was audio and video recorded and subsequently transcribed for qualitative analysis. The analysis was conducted using MAXQDA, a specialist software platform for qualitative and mixed-methods research widely used in social science and design research contexts (VERBI Software, 2023). MAXQDA was used to code the session transcript systematically, enabling both the attribution of individual contributions to specific participants and the identification of recurring themes across the full dataset.

Table 1 presents the participant profiles, speaker codes (Speaker 1-7) correspond to the speaker identifiers assigned during MAXQDA coding and are used consistently throughout this paper to attribute contributions. All participants who attended provided informed consent for the recording and use of workshop data for research purposes, in accordance with a recording notice and consent form distributed prior to the session.

 doi:10.20944/preprints202603.1128.v1

Table 1. Participant profiles in the ABCDE pilot study (speaker codes correspond to MAXQDA transcript coding identifiers).

Speaker	Code	Professional Role	Area of Expertise	Relationship to Product
Speaker 1	AC	PhD Candidate-Researcher / Facilitator	IoT privacy, human-centred design, industrial design	External- study lead
Speaker 2	DH	Digital Part Engineer	Connected features, cooktops digital integration	Internal- digital engineering
Speaker 3	BS	Product Manager (UX & Accessibility)	Mobile apps, user experience, AI-driven solutions, accessibility	Internal-UX and feature ownership
Speaker 4	SA	Product Manager (IT)	Privacy compliance, data governance, onboarding flows, GDPR	Internal- IT product ownership
Speaker 5	AH	Analytics Product Manager	In-app analytics, data collection architecture, user behaviour tracking	Internal- data analytics ownership
Speaker 6	JD	Programme Manager (Operations)	Platform operations, cross-functional coordination, programme governance	Internal- operational management
Speaker 7	EM	Researcher 2 / Co-facilitator	IoT privacy, human-centred design, industrial design	External- research co-facilitator

Note. Own elaboration.

The research team was composed of AC (Speaker 1), the PhD candidate responsible for developing and leading the ABCDE Privacy Framework study, who served as the primary facilitator throughout the session; and EM (Speaker 7), a co-researcher who provided technical support and contributed to the live radar chart construction during the conclusions phase. The five industry participants (Speakers 2-6) represented a genuinely multidisciplinary cross-section of the organisation's product development structure, encompassing user experience, data analytics, platform operations, software engineering, and regulatory compliance perspectives. The workshop was conducted entirely online via a video conferencing platform, reflecting the distributed nature of the team across different European offices. This online modality was treated as a fully valid configuration of the framework's application protocol, and its practical implications are discussed in this paper.

2.2. Before the Workshop: Preparation Phase

Consistent with the ABCDE Privacy Framework, a preparation and alignment session was conducted approximately one week prior to the main workshop. This session, lasting between 20 and 30 minutes, was attended by both members of the research team (AC and EM) and all participants who would take part in the subsequent workshop.

The preparation session served three principal objectives. First, it introduced participants to the structure and objectives of the ABCDE Privacy Framework, its conceptual origins in Nielsen's usability heuristics (Nielsen, 1994) and the PbD paradigm (Cavoukian, 2009), its application protocol, and the intended outputs of the workshop session. Participants were informed that the session was designed to surface shared professional perceptions of privacy usability rather than to produce a formal compliance audit, and that divergent perspectives across roles would be methodologically valuable rather than indicative of error.

Second, the session established the use case and user scenario that would anchor the main workshop. The scenario was negotiated during the session to ensure both its relevance to the

 doi:10.20944/preprints202603.1128.v1

participants' product context and its coverage of the privacy-relevant moments in the application's user journey. The agreed use case was as follows: a family of four has recently purchased a new connected dishwasher. One of the parents downloads the IoT companion application, completes the registration and onboarding process, configures permissions and notification preferences, pairs the dishwasher with the app, and subsequently uses the application to start the appliance remotely from their workplace using a smart scheduling or intelligent programme feature. The scenario was structured around three sequential interaction stages: (1) setup and onboarding, (2) remote use from work and (3) shared family use, acknowledging that within a shared household environment, multiple users may interact with the same connected appliance under different conditions, access levels, and degrees of awareness.

Third, the session assigned to each participant the two heuristics for which they would be responsible for initiating the discussion during Round 1. This assignment was a deliberate design decision embedded in the framework's protocol, motivated by the aim of ensuring that each heuristic discussion began from a position of individual preparation and role-specific ownership. Participants were encouraged to interact with the application in advance of the workshop, ideally by completing the registration and onboarding process with a test account or by drawing on their professional familiarity with the product. As seen in Figure 1 a set of scoring cards was distributed digitally for preparation purposes; in practice two of them performed the scoring using hand signals during the video call.

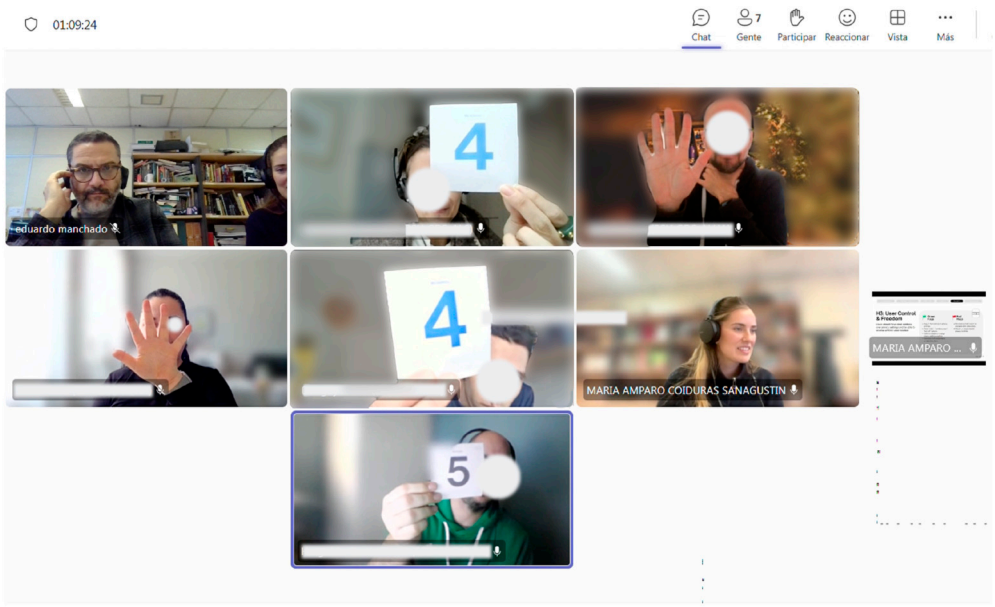


Figure 1. Online workshop session conducted via Microsoft Teams, showing participants voting on a privacy heuristic using physical score cards and hand gestures. Note. Screenshot captured during the pilot study session. Participant faces have been anonymised in accordance with confidentiality protocol.

2.3. Workshop Structure and Protocol

The main workshop was conducted on 12 December 2025, from 10:00 to 12:00, and lasted approximately two hours in total. The session was structured according to the ABCDE workshop protocol, comprising six sequential segments: introduction and agenda review, framework and tool overview, use case review, Round 1 (heuristic discussion), Round 2 (individual assessment), and conclusions and wrap-up. The protocol was implemented without material deviation from the planned structure, and the timing of each segment closely matched the allocations specified in the framework design.

 doi:10.20944/preprints202603.1128.v1

2.3.1. Introduction and Tool Overview

The opening segment (approximately ten minutes) was devoted to welcoming participants, confirming consent for session recording, completing participant introductions, and reviewing the session agenda. Participants stated their names, roles, and professional background within the organisation, providing a brief orientation that contextualised their subsequent contributions. The primary facilitator (AC) then presented a concise overview of the ABCDE Privacy Framework: its conceptual origins, its relationship to PbD principles and Nielsen's usability heuristics, and the specific objectives and anticipated outputs of the session. Participants were explicitly reminded that the workshop was designed to surface perceptions and generate a shared professional account of the application's privacy usability profile, not a formal compliance assessment and that divergent perspectives across professional roles were methodologically valuable.

A review of the use case (approximately five minutes) followed the framework overview. This segment generated immediate spontaneous discussion, most notably on the privacy implications of shared household accounts and the super-user role: the account-holder who completes the initial onboarding process acquires elevated data-access and device-management privileges that may not be readily apparent to secondary household members. DH (Speaker 2) observed, ahead of the formal heuristic rounds, that the decision of which household member downloads and registers the application is itself a privacy decision with downstream consequences that users may not fully recognise. This observation foreshadowed several recurring themes in the subsequent heuristic discussions.

2.3.2. Round 1: Heuristic Based Discussion

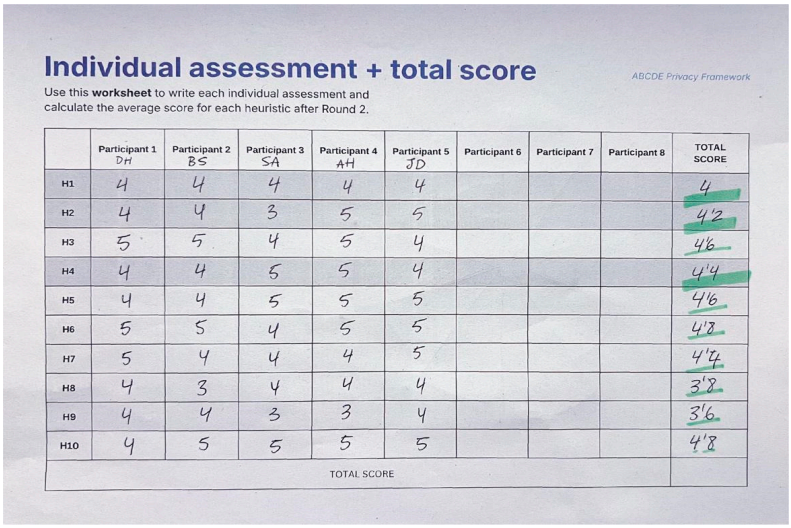
Round 1 constituted the core qualitative phase of the workshop and lasted 48 minutes, closely matching the planned 50-minute allocation and thereby confirming the validity of the time estimates embedded in the framework's protocol. Each of the ten privacy usability heuristics was addressed sequentially, with a maximum of five minutes per heuristic. For each slot, the facilitator (AC) read aloud the heuristic definition, its associated positive practices (green flags), and its associated risk patterns (red flags), before inviting the pre-assigned participant to open the discussion. Open contributions from all participants followed, with the facilitator managing pacing and ensuring that every heuristic received dedicated treatment.

The discussion format was conversational, associative, and explicitly non-evaluative. Participants were encouraged to draw on both their professional expertise and their direct experience of the application; both as product team members and as users. All oriented to ground their contributions in specific interface moments, flows, or features where possible. Screenshots were shared via the video call chat during several heuristic slots to anchor the discussion in particular interface evidence. The session produced a rich and substantive qualitative dataset across all ten heuristics, reflecting the participants' depth of product knowledge and their genuine engagement with the framework's analytical questions.

2.3.3. Round 2: Individual Assessment

Following a brief optional break, Round 2 was conducted as a rapid, structured scoring phase lasting approximately 20 minutes. Each of the five industry participants individually assigned a score from 0 to 5 to each of the ten heuristics, using the scoring rubric defined by the framework: 0 (not present / no evidence of privacy usability), 1 (very weak), 2 (weak-red flags predominate), 3 (acceptable-mixed evidence), 4 (good-green flags predominate), 5 (very strong-consistently best-practice). Scores were revealed simultaneously for each heuristic, with participants using the template given or hands with finger counts in the online video call setting. The research co-facilitator (EM) wrote in real time the scores given in this phase (Figure 2).

 doi:10.20944/preprints202603.1128.v1



Individual assessment + total score

ABCDE Privacy Framework

Use this **worksheet** to write each individual assessment and calculate the average score for each heuristic after Round 2.

	Participant 1 DH	Participant 2 BS	Participant 3 SA	Participant 4 AH	Participant 5 JD	Participant 6	Participant 7	Participant 8	TOTAL SCORE
H1	4	4	4	4	4				4
H2	4	4	3	5	5				4'2
H3	5	5	4	5	4				4'6
H4	4	4	5	5	4				4'4
H5	4	4	5	5	5				4'6
H6	5	5	4	5	5				4'8
H7	5	4	4	4	5				4'4
H8	4	3	4	4	4				3'8
H9	4	4	3	3	4				3'6
H10	4	5	5	5	5				4'8
TOTAL SCORE									

Figure 2. Individual assessment written during the pilot study workshop. Note. Own elaboration.

Brief deliberation followed any heuristic where notable divergence in individual scores was observed. In most cases, participants were closely aligned, which AC noted during the session as evidence that the Round 1 qualitative discussion had produced genuine convergence of understanding, not premature social consensus, but a shared evaluative framing grounded in the specific evidence discussed. Where lower scores were given, participants explained their reasoning voluntarily, contributing additional qualitative insight that enriched the interpretation of the quantitative profile.

2.3.4. Conclusions of the Workshop

The final segment of the workshop was devoted to generating average scores for each heuristic and constructing the radar chart collaboratively. EM (Speaker 7) led the numerical computation and live chart drawing in a shared graphical environment, while AC facilitated the group reflection that developed as the visualisation took shape. This collaborative construction was a deliberate methodological choice embedded in the framework's design. So, making the synthesis visible and immediate, the radar chart functioned not merely as *a posteriori* reporting device but as a conversational artefact within the session, prompting interpretive commentary as it emerged and enabling participants to observe their own collective assessment in real time. The session concluded with individual verbal reflections from participants on the value of the exercise, followed by a reminder regarding the post-session online questionnaire.

3. Results

3.1. Qualitative Findings: Heuristic-by-Heuristic Analysis

The following section presents the key themes and findings from the Round 1 qualitative discussion, organised by heuristic. Participant contributions are attributed by speaker code to preserve individual anonymity while retaining the relational context of the discussion. Direct quotations are drawn from the session transcript and have been lightly edited for readability without alteration of meaning.

H1: Visibility of System *Status*

Discussion of this heuristic centred on the onboarding and registration flow as the primary moment at which the application communicates its privacy state to the user. BS (Speaker 3) identified account creation as a critical privacy juncture, this is the point at which personal data, including name and email address, is first transmitted to and stored on the company's infrastructure.

The discussion established a productive distinction between privacy visibility during onboarding (characterised as partially adequate) and privacy visibility during ongoing use (assessed

 doi:10.20944/preprints202603.1128.v1

as generally good), a temporal differentiation that constitutes one of the central tensions in the application's privacy usability profile.

H2: Match Between System and Real World

This heuristic generated sustained discussion about the contrast between different layers of privacy communication within the application. SA (Speaker 4) raised a concern about the comprehensibility of the full legal documentation. Particularly, the data privacy policy presented as a linked PDF. While the document is structurally organised, SA described it as potentially relying on technical and legal jargon that, while formally necessary, presents a genuine comprehension barrier for non-specialist users. BS (Speaker 3) reinforced this observation, contrasting the concise analytics opt-in, "a 30-second read", with the full legal document, which "you would need a couple of minutes to understand". SA further noted, that the majority of users accept privacy agreements without reading them, a finding that directly validates one of the central concerns motivating the present doctoral research.

H3: User Control and Freedom

This heuristic received the strongest initial agreement and produced the least contested discussion of the session. AH (Speaker 5) described the privacy settings architecture as well-structured and accessible, consistent with the requirements of Articles 7 and 17 of the General Data Protection Regulation (European Parliament & Council of the European Union, 2016).

The primary qualification raised concerned the account deletion flow, which while accessible, requires navigation through a different section from the main privacy settings. A second area of discussion concerned the asymmetry between the super-user and secondary user roles, while both account types can access privacy settings within their own profiles, only the super-user controls the initial device pairing and its associated data access permissions, and this asymmetry may not be evident to users who are subsequently added as secondary household members.

H4: Consistency and Standards

SA (Speaker 4) led the discussion for this heuristic, observing that the centralisation of all privacy-related content within a single settings section produces strong internal consistency. Privacy controls, legal documents, data collection settings, and related information are grouped in one location using consistent terminology, iconography, and structural organisation.

SA also raised a productive open question: whether this concentration in a single dedicated section, while internally consistent, may render privacy invisible during the rest of the user experience. The application does not surface privacy-relevant signals contextually, for example, at the moment a user enables a new feature requiring additional data access, or during the execution of appliance programmes that generate usage data. This tension between consistency through centralisation and the need for contextual privacy signalling was identified as a design opportunity and recurred as one of the most analytically generative themes of the session.

H5: Error Prevention

Discussion of error prevention in the privacy context identified two clear areas of strength.

An area for improvement was identified by AC (Speaker 1), who noted that some applications implement confirmation prompts or scroll-to-unlock mechanisms at privacy-sensitive commitment moments, requiring users to engage actively with privacy information before proceeding, rather than allowing automatic progression. BS responded that this pattern is familiar but uncommon: "I've seen this in a lot of video games. You need to scroll all the text but no one reads it. But they force you somehow to think about what you're doing". The group agreed that even if such mechanisms do not guarantee comprehension, they introduce a reflective moment that may reduce inadvertent or unconsidered consent.

 doi:10.20944/preprints202603.1128.v1

H6: Recognition Rather than Recall

This heuristic received the highest average score of the session and was the subject of the most rapid and uncontested discussion, reflecting a high level of participant consensus about the application's performance on this dimension.

BS (Speaker 3) shared screenshots demonstrating that the privacy settings section is visually distinguished from the rest of the application settings through a distinct colour treatment and clear, self-explanatory labelling, a design choice that allows users to locate privacy controls without memorising navigation paths.

H7: Flexibility and Efficiency of Use

JD (Speaker 6) opened the discussion for this heuristic by noting that privacy settings are accessible and modifiable regardless of user role, both super-users and secondary users have access to the same privacy controls within their respective account profiles. The facilitator (AC) reframed the heuristic to emphasise the expert/novice distinction, the application provides a layered information architecture in which users can engage with short, plain-language summaries of privacy settings or navigate deeper into full legal documentation if they wish, a structure that partially accommodates different levels of interest in, and capacity for, privacy-related engagement.

The discussion converged on the observation that the application provides reasonable flexibility for individual privacy management while offering limited support for the complexity of shared-household privacy preferences, a gap that becomes particularly significant in the domestic IoT contexts for which the framework is designed.

H8: Aesthetic and minimalist design

This heuristic produced the most divergent discussion of the session and received the second-lowest average score, reflecting genuine disagreement across participant perspectives. AH (Speaker 5) praised the visual clarity of the privacy settings interface. BS (Speaker 3), however, introduced a distinction between the main part of the app, whereas the full data privacy document, presented as a lengthy PDF containing dense legal text, clearly exemplifies the red flag of long blocks of dense privacy text.

This asymmetry was acknowledged by all participants. BS observed: "*We could make it better by having this long text a little bit shortened and then there's another link if you want to see the full information*". SA added that internal consumer research consistently confirmed that the majority of users accept privacy documentation without reading it, describing the dense legal text as something users "*don't understand*" and therefore avoid entirely. This observation validates the central concern of the Transparency Asymmetry theme identified in the coding analysis.

H9: Help Users Recognise, diagnose, and recover from errors

This heuristic generated the richest and most expansive discussion of the session, produced the lowest average score, and surfaced several issues of genuine strategic and regulatory relevance to the participating team. SA (Speaker 4) broadened the framing from appliance errors to privacy errors, noting that forthcoming European cybersecurity regulations would require companies to notify users in the event of personal data breaches: *"From next January on, it will be operative the European cybersecurity agreement, and we will be forced to inform all our users if this happens"*. This regulatory horizon raised important design questions about how to communicate the severity and nature of a privacy incident in a calibrated way, distinguishing serious breaches from minor notifications, and doing so without generating either disproportionate alarm or insufficient urgency.

DH (Speaker 2) contributed an important conceptual distinction, many products communicate error states of significantly different severity using the same visual language and alarm level, leaving users unable to assess actual urgency. The same dynamic applies to privacy errors. BS (Speaker 3) connected this to the super-user scenario: "*The super-user situation might be one of those things where we need to be really clear about what the customer is doing and also if he did this wrong, he can revert this invitation*". The gap between the existence of a corrective mechanism and its discoverability at the

 doi:10.20944/preprints202603.1128.v1

moment it is needed was identified as a priority area for improvement, and one that will become particularly consequential under forthcoming EU data breach notification obligations.

H10: Help and documentation

The final heuristic also received the highest average score, tied with H6. AH (Speaker 5) expressed surprise at the depth of documentation available within the application's settings section: "*I find it very positive that the parts are separated from the legal text and the explanation. There is not a lot of text. It's very easy to read*". SA (Speaker 4), who led the discussion for this heuristic, was similarly surprised by the level of transparency, noting that the settings section includes not only data privacy and terms-of-use documents but also detailed technical information about third-party software libraries used in the application, a level of transparency not previously noticed despite professional familiarity with the product.

Both DH (Speaker 2) and BS (Speaker 3) noted that the primary limitation under this heuristic was not the availability of documentation but its format, density, and navigability. Task-oriented guidance, for example, instructions for how to manage device permissions, revoke a secondary user's access, or understand the implications of a particular data collection setting, is largely absent, replaced by comprehensive but difficult-to-navigate legal documents. The consensus was that the application provides extensive documentation but would benefit significantly from better visual organisation, progressive disclosure techniques, and contextually embedded help.

3.2. Qualitative Analysis: Thematic Coding and MAXQDA Visualisation

In addition to the heuristic-by-heuristic account presented previously, the qualitative data generated during the workshop was subjected to systematic thematic coding analysis using MAXQDA qualitative data analysis software (VERBI Software, 2023). The aim of this analysis was twofold: (i) to identify recurrent themes and conceptual patterns that cut across multiple heuristics, offering a higher-level characterisation of the application's privacy usability profile; and (ii) to evaluate the ABCDE Privacy Framework as an analytical instrument, specifically with respect to its capacity to surface substantive and design-relevant findings from structured team discussion.

The coding procedure followed a hybrid approach combining deductive and inductive elements (Braun & Clarke, 2006). A first pass of the session transcript generated descriptive, first-order codes closely anchored to participant words. A second pass grouped these codes into interpretive, second-order themes reflecting conceptual patterns across the data. A final analytic pass identified aggregate dimensions characterising the overarching structure of the privacy usability profile. The full session was transcribed *verbatim*, with speaker attribution maintained throughout using the MAXQDA speaker codes listed in Table 2. Figure 3 presents a word cloud generated from the transcript, providing a lexical overview of the discussion that precedes the systematic coding analysis.

 doi:10.20944/preprints202603.1128.v1

Figure 3. Word cloud generated from the pilot study session transcript. Term size reflects relative frequency of occurrence across the complete transcript. Note: Own elaboration using MAXQDA (VERBI Software, 2023).

The dominant terms in the word cloud were: privacy, user, heuristic, information, data, legal, personal, appliance, document, and access. All of them reflect the three conceptual registers that structured the session: (1) the substantive domain under assessment (privacy, personal data, appliance), (2) the analytical vocabulary introduced by the ABCDE Privacy Framework (heuristic, flag, assessment), (3) and the product-specific discourse of the participating team (account, settings, screen, connect, dishwasher). The co-presence of terms from the legal-compliance register (legal, document, compliance) alongside terms from the experiential register (user, clear, access, control) is consistent with the Transparency Asymmetry theme (T1) identified in the coding analysis, the discussion navigated persistently between the technical-legal language of formal compliance and the experiential language of user-centred design. The word cloud thus provides a high-level confirmation of the thematic landscape that the systematic coding process maps in greater analytical detail below. Table 2 presents an illustrative selection of first-order codes derived from the coding process, alongside their thematic assignment and supporting evidence from the transcript.

Table 2. Illustrative first-order codes derived from MAXQDA transcript analysis, with supporting evidence and thematic assignments.

Code ID	First-Order	Representative Quote (transcript)	Theme	H#
C-01	Transparency asymmetry between opt-in and legal document	"When we do the opt-in we do it better... but with the account creation, you end up in a long document" (BS, Speaker 3)	T1	H1, H2, H8
C-02	Two-click access to privacy settings	"Those are about two clicks away... you go into the settings and then it's very structured" (AH, Speaker 5)	T2	H1, H6
C-03	Privacy absent from in-app journey outside settings	"Perhaps to have only the point in one single point is not visible enough" (SA, Speaker 4)	T2	H4, H1
C-04	Super-user role creates household privacy asymmetry	"Which one of the two parents will be responsible... this is a decision about privacy" (DH, Speaker 2)	T3	H3, H7, H9
C-05	Proactive disclaimers at free-text fields	"Those input fields have a clear disclaimer above them: don't share any personal information" (BS, Speaker 3)	T4	H5
C-06	No scroll/confirmation friction at commitment moments	"I've seen this in a lot of video games... that we don't use. That's correct" (BS, Speaker 3)	T4	H5
C-07	EU cybersecurity regulation demands calibrated error communication	"From next January on... we will be forced to inform all our users" (SA, Speaker 4)	T5	H9
C-08	Users systematically skip legal privacy documentation	"A majority of them really don't read it. They say yes, I accept it without reading" (SA, Speaker 4)	T1	H2, H8
C-09	Positive surprise at documentation depth	"I was even surprised how many documents and how much transparency we have" (SA, Speaker 4)	T2	H10
C-10	Workshop surfaces cross-role alignment on privacy	"We are on the same page here... I guess we are quite well aligned" (BS, Speaker 3)	T6	Framework

Source: own elaboration using MAXQDA.

 doi:10.20944/preprints202603.1128.v1

Five second-order themes were identified, and a sixth emerged from the methodological dimension of the session:

Theme 1 (T1): Transparency asymmetry.

This theme captures the consistent pattern, observable across H1, H2, and H8, whereby the application demonstrates exemplary, user-centred privacy communication in specific, bounded contexts (particularly the analytics opt-in flow) while relying on dense, rarely-read legal documentation for its broader formal disclosures. The tension between these two modes of communication represents a structural inconsistency with practical implications for the quality of users' informed consent (Solove, 2006).

Theme 2 (T2): Centralised but decontextualised privacy.

Prominent across H4, H1, H6, and H10, this theme characterises the application's approach of concentrating all privacy-related controls and documentation within a single, well-organised settings section. While this produces strong internal consistency and high accessibility scores on H6 and H10, it also means that privacy is structurally absent from the interaction contexts in which privacy-relevant actions actually occur. Privacy visibility is available on demand but not proactively surfaced.

Theme 3 (T3): Shared household complexity.

Most prominently associated with H3, H7, and H9, this theme captures the distinctive privacy dynamics introduced by the shared household use case. The super-user architecture assigns the account-holder who completes initial onboarding an elevated level of device-management and data-access control that is not voluntarily apparent to secondary household members, creating privacy asymmetries specific to the domestic IoT context.

Theme 4 (T4): Reactive rather than preventive privacy design.

Across H5 and related discussion threads, the analysis revealed a broader pattern in which the application's privacy design is primarily reactive, providing corrective mechanisms when users seek them, rather than preventive, introducing friction or prompts at the moments where privacy-relevant commitments are made. The absence of confirmation mechanisms at onboarding and of contextual privacy alerts reflects a design philosophy that prioritises efficient user flows over deliberate privacy engagement.

Theme 5 (T5): Regulatory horizon and error communication readiness.

Discussion of H9 surfaced an important forward-looking dimension; participants' awareness of forthcoming EU regulatory requirements under the European Cybersecurity Act generated substantive debate about whether the current error communication design is adequate for guiding privacy-specific incidents with appropriate severity differentiation. This theme points to a gap between current design practice and emerging regulatory demands that will require proactive investment.

Theme 6 (T6): The workshop as alignment mechanism.

A methodological theme emerged not from the evaluated product but from the session's own dynamics. Multiple moments in the transcript, and the explicit closing reflections from participants, indicated that the structured heuristic discussion enabled the team to surface shared knowledge and reach cross-role alignment on privacy usability issues that had not previously been collectively articulated. This function, the workshop as a vehicle for privacy-relevant knowledge sharing, represents an organisational value that complements its more direct analytical outputs.

Figure 4 presents a word frequency trend analysis generated in MAXQDA, tracking the absolute frequency of four conceptually significant terms, privacy, user, heuristic, and legal, across the ten sequential sections of the workshop transcript, each corresponding to one heuristic discussion slot. This visualisation complements the static word cloud by revealing how the discourse evolved across the session.

 doi:10.20944/preprints202603.1128.v1

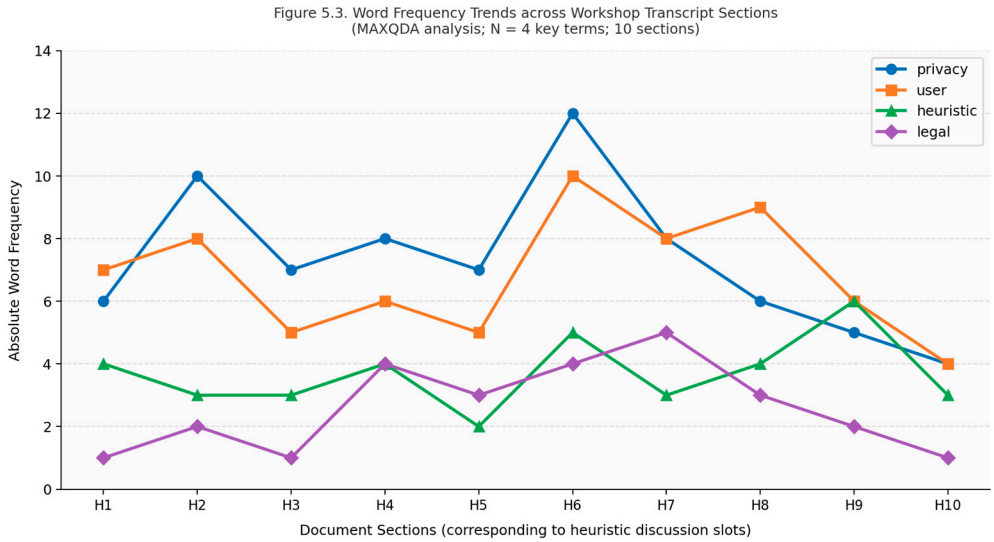


Figure 4. Word frequency trend across the ten heuristic discussion sections of the workshop transcript (H1–H10 on x-axis; absolute frequency on y-axis). Note: Own elaboration using MAXQDA (VERBI Software, 2023).

The term "privacy" reaches its highest absolute frequency in H2 (Match Between System and Real World) and H6 (Recognition Rather than Recall), reflecting the concentrated substantive richness of those heuristic slots, both of which generated the most sustained and direct engagement with the privacy implications of the application's interface architecture. The term "legal" shows a marked peak in the H4, H6 and H7 sections, consistent with the discussions of documentation density, legal-format privacy policies, and formal compliance that dominated those portions of the session. The term "heuristic" increases in frequency towards the latter sections of the transcript, corresponding to Round 2 scoring and the closing reflection, when participants engaged more explicitly with the framework's evaluative vocabulary. The term "user" remains relatively constantly present throughout the session, underscoring the degree to which the discussion maintained an experiential, user-centred orientation across all ten heuristics rather than retreating into purely technical or regulatory frames. Together, these trends corroborate the thematic coding analysis by demonstrating that the conceptual tensions identified, particularly between legal-compliance discourse and user-centred design thinking, were not restricted to individual heuristic slots but distributed across the full arc of the session, confirming their status as structural features of the workshop discussion.

3.3. Quantitative Results: Individual Scores, Averages and Radar Chart

Following the qualitative discussion phase, the five industry participants individually assigned scores to each heuristic using the 0–5 scale defined in the ABCDE Privacy Framework. Scores were revealed simultaneously for each heuristic and the arithmetic mean was calculated in real time by EM (Speaker 7). Table 3 presents the resulting average scores.

Table 3. Average heuristic scores assigned by the five industry participants (scale 0–5; n=5). Performance levels correspond to the ABCDE Privacy Framework scoring rubric.

Code	Heuristic	Average Score (0–5)	Performance Level
H1	Visibility of system Status	4.0	Good
H2	Match between system and real World	4.2	Good
H3	User control and freedom	4.6	Good-Strong
H4	Consistency and standards	4.4	Good
H5	Error prevention	4.6	Good-Strong
H6	Recognition rather than recall	4.8	Strong
H7	Flexibility and efficiency of use	4.4	Good

 doi:10.20944/preprints202603.1128.v1

H8	Aesthetic and minimalist design	3.8	Acceptable–Good
H9	Help Users recognise, diagnose, and recover from errors	3.6	Strong
H10	Help and documentation	4.32	Good

Note: own elaboration.

The quantitative profile reveals a coherent and internally consistent pattern. The application performs strongly on dimensions related to the accessibility and discoverability of privacy controls (H6: 4.8; H10: 4.8), user autonomy and reversibility (H3: 4.6; H5: 4.6), and structural consistency (H4: 4.4). These high scores map precisely onto the strengths identified through qualitative analysis and the word frequency trends in Figure 4. The centralised, well-organised privacy settings architecture; the clear toggle mechanisms for managing data collection preferences; and the explicit disclaimers at free-text input points. The scores on H6 and H10 in particular suggest that, on dimensions of findability and documentation coverage, this IoT companion application performs at a level that notes the frequently negative characterisation of privacy design in IoT contexts reported in the existing literature (Coiduras-Sanagustín et al., 2024; Emami-Naeini et al., 2017).

The weakest dimensions are H9 (3.6) and H8 (3.8). Both reflect limitations identified through qualitative analysis. They are consistent with the T1: Transparency asymmetry and T5: Regulatory Horizon themes, the reliance on dense legal documentation (H8) and the absence of calibrated privacy-error communication and recovery pathways (H9). These two heuristics also generated the greatest discussion time and the most voluntary participant elaboration during Round 1. This indicates that they were perceived as areas of genuine design concern. The overall mean score of 4.32 indicates that the evaluated application performs at a generally good level across the full spectrum of ABCDE Privacy Framework dimensions. While the variance within the profile, particularly the pronounced gap between H9 and H6/H10, provides specific and actionable design priorities for the participating team.

Figures 5 and 6 presents the radar chart constructed during the workshop session (physically and digitally), visualising the distribution of average scores across all ten heuristics. The chart makes the profile of strengths and relative weaknesses immediately legible to a non-specialist audience, consistent with the framework's design goal of producing communicable outputs that can travel beyond the session itself.

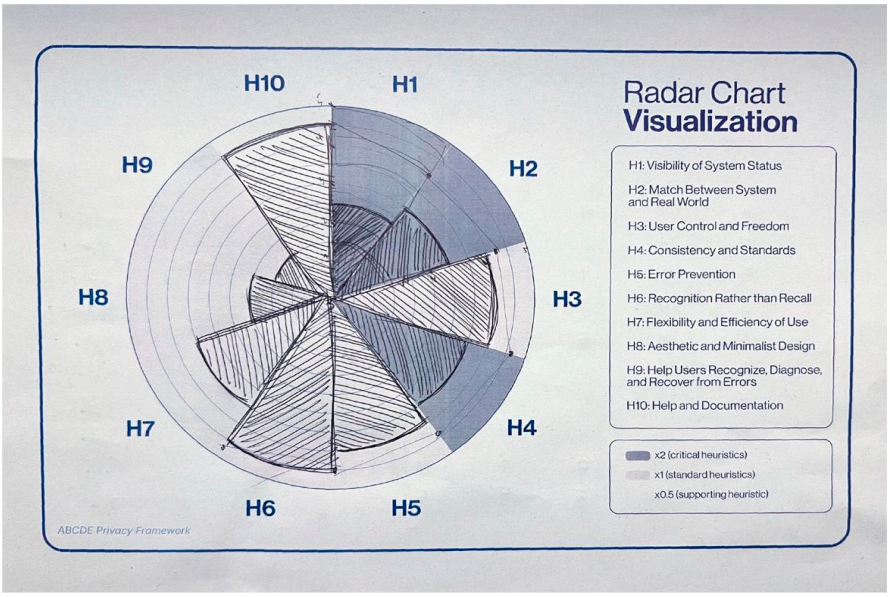


Figure 5. Privacy usability radar chart creation for Company X in paper (ABCDE Privacy Framework Assessment, 12 December 2025). Note. Live elaboration during the workshop in paper.

 doi:10.20944/preprints202603.1128.v1

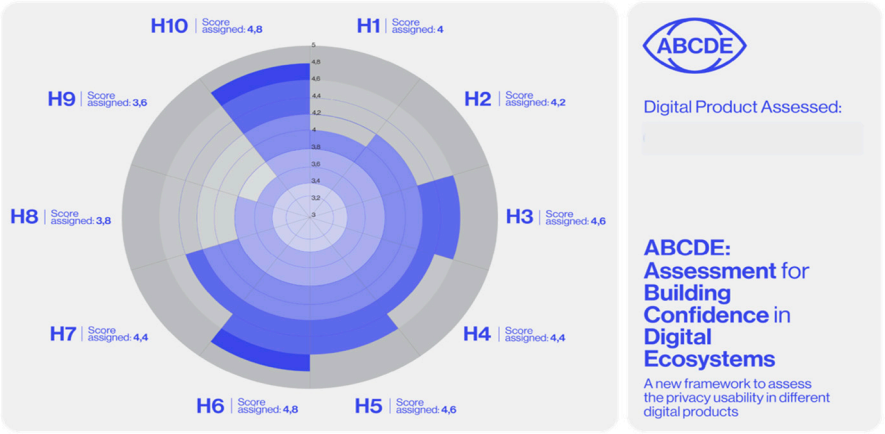


Figure 6. Privacy usability radar chart creation for Company X (ABCDE Privacy Framework Assessment, 12 December 2025). Note: Live elaboration during workshop digitally(ABCDE Privacy Framework Assessment, 12 December 2025).

The live construction of the radar chart during the session generated immediate interpretive commentary. BS (Speaker 3) noted that the visual representation made the relative weakness of H8 and H9 more legible than the numerical table had done alone. DH (Speaker 2) observed that the chart showed "our shared appreciation of what is the situation of your digital product regarding the privacy of the users" and proposed that the same framework could be applied to a competitor's product and the results compared. An observation that suggests participants were already conceptualising extensions of the framework beyond the immediate session context. This response confirms the framework's design rationale for using radar chart visualisation as a synthesis and reflection tool rather than merely a reporting device.

3.5. Participant Feedback and Methodological Observations

The verbal reflections offered by participants at the close of the workshop constitute the primary source of evaluative feedback on the ABCDE Privacy Framework. Despite the constraints of the online format and the demands of a two-hour session, all five industry participants offered spontaneous closing reflections without prompting and the substantive quality of these contributions suggests a level of genuine engagement with the exercise. SA (Speaker 4) offered what is perhaps the most direct formulation of the framework's perceived value: "I found it very practical, very straightforward, and going to really important points that perhaps we don't have in our agenda every day". This observation points to a structural feature of professional product development contexts. The tendency for privacy considerations to be addressed reactively, under regulatory pressure, rather than as a routine object of team reflection and positions the ABCDE Privacy Framework as a mechanism capable of creating structured space for precisely this kind of deliberation. JD (Speaker 6) articulated the same insight from a slightly different angle, noting that the workshop had enabled the team to engage with privacy "not because it is suddenly a big problem or suddenly a priority", but as a proactive and legitimate use of professional time, a reframing that is itself non-trivial in organisational contexts where privacy tends to be treated as a compliance function rather than a design one.

A second dimension of the participant feedback concerns the conceptual broadening effect of the framework. Its capacity to expand participants' understanding of what privacy usability encompasses beyond the legally outstanding categories that typically anchor both professional and amateur conceptions of privacy. DH (Speaker 2) gave this the most explicit formulation: "Usually when I thought about this kind of topic, I thought: my personal data, the name, the credit card. But it's true that there are other things that we need to take into account". This acknowledgement, from a digital engineer with nearly three years of product experience, suggests that the ABCDE Privacy

 doi:10.20944/preprints202603.1128.v1

Framework's heuristic structure, by directing attention to dimensions such as contextual visibility, error communication calibration, and shared-household privacy asymmetries, succeeded in surfacing aspects of privacy usability that professional routines had not previously made noticeable. SA (Speaker 4) reinforced this point from an organisational perspective, observing that the session helped the team "understand other perspectives, because as we have seen, we are not all on the same page for all these aspects and all these heuristics". This cross-role misalignment, revealed precisely through the structured dialogue the framework facilitates. It is not a weakness of the team but a predictable consequence of the functional specialisation inherent in multidisciplinary product development; the framework's value lies in making these divergences visible and productive.

A third dimension emerging from the closing reflections concerns the perceived scalability and strategic utility of the framework's outputs, particularly the radar chart produced during the session. DH (Speaker 2), drawing directly on the visual artefact, described the chart as offering "your shared appreciation of what is the situation of your digital product regarding the privacy of the users", and immediately proposed a series of extensions:

- applying the same framework to a competitor's product to enable comparative benchmarking
- commissioning an external advisor to conduct the same assessment independently
- allowing for a comparison of expert and internal team perspectives and
- repeating the exercise with different team compositions to surface alternative viewpoints.

These suggestions, offered spontaneously, without prompting, by a participant with no prior familiarity with the framework, indicate that the ABCDE Privacy Framework's outputs were experienced not as a terminal deliverable but as a starting point for ongoing strategic engagement with privacy usability. The radar chart, appears as a representational artefact sufficiently flexible to be interpreted across professional roles yet sufficiently robust to anchor a shared conversation about design priorities, improvement directions, and competitive positioning.

In terms of methodological observations, the research team noted that the pre-assignment of discussion initiators per heuristic was highly effective in maintaining session pace and avoiding conversational hesitation. Also, the absence of printed scoring cards in two participant cases did not weaken Round 2, as raised hand finger signals in the video call served as an adequate and friction-free substitute. The 48-minute duration of Round 1 closely matched the 50-minute planned allocation, and the almost 20 minutes for Round 2 also validated the time estimates in the protocol.

4. Discussion

The pilot study demonstrates that the ABCDE Privacy Framework can be successfully implemented in a real industrial context. The session produced a rich qualitative dataset and quantitative assessment that were the base for the later interpretive discussion.

Several aspects of the framework's performance need particular discussion. First, Round 1 discussions enriched the interpretation of Round 2 scores. Participants' explanations of lower scores on H8 and H9 provided design-relevant rationale that numbers alone could not have conveyed. Equally, the scoring phase introduced a degree of precision that the discussion alone could not have produced, enabling the construction of the radar chart and the identification of other priorities. The MAXQDA visualisations further enriched this analytical integration by revealing patterns in the discourse structure. Particularly, the distribution of legal-register and user-register vocabulary across heuristic slots that are not visible from a heuristic-by-heuristic reading alone.

Second, the framework proved effective at surfacing latent knowledge within the participating team. Several design issues identified during the session, including the communicative gap between the opt-in screen and the full privacy document. Also, the risk-communication challenges of H9 in relation to forthcoming regulatory requirements, and the contextual invisibility of privacy-relevant events during routine app use, were familiar to individual participants but had not been systematically articulated or collectively addressed. The heuristic structure provided a shared

 doi:10.20944/preprints202603.1128.v1

language and a bounded conversational space in which these observations could be raised, compared, and connected across professional roles.

Third, the pilot study produced findings with broader relevance to the privacy usability research agenda. The high scores on H6 and H10 suggest that at least some IoT companion applications perform well on the dimensions of privacy controls accessibility and documentation coverage. The lower scores on H8 and H9, meanwhile, point to persistent design tractable challenges in communicating privacy information at a level appropriate for general users rather than legal professionals (Solove, 2006) .

4.1. Limitations

Several limitations of the present pilot study should be acknowledged. First, the study involved a single industrial partner and a single digital product, which restricts both the generalisability of the substantive findings and the applicability of the methodological observations. The framework's robustness across different product types, organisational cultures, team compositions, and national regulatory contexts remains to be established through multi-site applications.

Second, the assessment was conducted exclusively by industry professionals with expert knowledge of the evaluated product. While this professional perspective is analytically valuable, it differs in important ways from the perspective of general end users, who may encounter the same interface with different mental models, lower product familiarity, and different privacy expectations. The optional user-centred phase of the ABCDE Privacy Framework, involving semantic differential scales with end users, was not implemented in this pilot study and represents a significant direction for future empirical work.

Third, as an entirely online session, the workshop could not make use of the physical scoring artefacts anticipated by the in-person protocol. Future work should investigate whether physical artefacts enhance the engagement, reflective quality, or collaborative experience of the scoring phase in face-to-face settings, particularly with larger participant groups.

Finally, the thematic coding analysis was conducted by a single researcher. Inter-rater reliability was not formally assessed at this stage. Future applications of qualitative coding to ABCDE Privacy Framework session transcripts should consider multi-rater procedures and formal reliability measures to strengthen the analytical rigour of the coding process (Braun & Clarke, 2006).

5. Conclusions

This study has presented an industrial pilot application of the ABCDE Privacy Framework, conducted as a structured two-hour workshop with a multidisciplinary team of seven participants; five industry professionals from Company X and two members of the research team on 12th of December 2025. The session assessed the privacy usability of the company's IoT companion application.

The session produced a rich qualitative dataset, analysed both heuristic by heuristic and through systematic thematic coding supported by MAXQDA visualisations. Five second-order themes were identified: Transparency asymmetry (T1), Centralised but decontextualised privacy (T2), Shared household complexity (T3), Reactive rather than Preventive privacy design (T4), and Regulatory horizon and Error communication readiness (T5). A sixth methodological theme, the workshop as alignment mechanism (T6), emerged from the session's own dynamics, with implications for the framework's value as an organisational learning tool beyond its direct analytical outputs.

The MAXQDA word cloud (Figure 3) and word frequency trend analysis (Figure 4) provided visual corroboration of these themes, confirming that the tension between legal-compliance discourse and user-centred design thinking was not confined to individual heuristic slots but constituted a structural feature of the workshop discussion as a whole.

The quantitative assessment produced average heuristic scores ranging from 3.6 (H9: Help users recognise, diagnose, and Recover from errors) to 4.8 (H6: Recognition rather than recall; H10: Help and documentation), with an overall mean of 4.32. The radar chart (Figures 5 and 6), constructed

 doi:10.20944/preprints202603.1128.v1

collaboratively during the session by the research team, made the distribution of strengths and relative weaknesses immediately legible, prompting productive interpretive reflection from participants and serving as a tangible, communicable output for the team.

The pilot study demonstrates that the ABCDE Privacy Framework is feasible, time-efficient, and analytically productive in an industrial context. It generated substantive relevant insights for design and for the participating organisation and methodological observations. Also including the effectiveness of the pre-assignment protocol, the suitability of online adaptations, and the value of the live radar chart construction, that will inform future applications and the continued development of the framework.

The findings from this study advance that privacy usability evaluation can be operationalised in industrial settings without prohibitive resource requirements, and that structured, heuristic-based assessment processes can function not only as diagnostic tools but as vehicles for professional learning, cross-role alignment, and PbD thinking within product development teams.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Agencia Española de Protección de Datos (AEPD) (Ed.). (2019). *A Guide to Privacy by Design*. https://www.aepd.es/guides/guide-to-privacy-by-design.pdf

Akrich, M. (1992). The de-scription of technical objects. *En W. Bijker & J. Law (Eds.), Shaping Technology/Building Society: Studies in Sociotechnical Change (Pp. 205-224). MIT Press.*

Al-Ghuwairi, A.-R., Al-Fraihat, D., Sharrab, Y., Alrashidi, H., Almujally, N., Kittaneh, A., & Ali, A. (2023). *Visualizing software refactoring using radar charts*. Nature. www.nature.com/scientificreports

Apthorpe, N., Reisman, D., & Feamster, N. (2017). *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic* (arXiv:1705.06805). arXiv. https://doi.org/10.48550/arXiv.1705.06805

Ardent Privacy. (2025). *Privacy by Design*. Https://Www.Ardentprivacy.Ai/Blog/the-7-Principles-of-Privacy-by-Design/. https://www.ardentprivacy.ai/blog/the-7-principles-of-privacy-by-design/

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*, *22*(7), 97–114.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. John Wiley & Sons.

Böhme, R., & Köpsell, S. (2010). Trained to Accept? A Field Experiment on Consent Dialogs. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2403–2406. https://doi.org/10.1145/1753326.1753689

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brown, A. J. (2020). "Should I Stay or Should I Leave?": Exploring (Dis)continued Facebook Use After the Cambridge Analytica Scandal. *Social Media + Society*, *6*(1), 205630512091388. https://doi.org/10.1177/2056305120913884

Brown, T. (2008). Design Thinking. *Harvard Business Review*, *86*(6), 84.

Brush, A. J. B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., & Dixon, C. (2011). Home automation in the wild: Challenges and opportunities. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11*, 2115–2124. https://doi.org/10.1145/1978942.1979249

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Cavoukian, A. (2009). Privacy by Design The 7 Foundational Principles. *Information and Privacy Commissioner of Ontario, Canada.*

 doi:10.20944/preprints202603.1128.v1

Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. *IEEE Consumer Electronics Magazine*, *9*(2), 78–82. IEEE Consumer Electronics Magazine. https://doi.org/10.1109/MCE.2019.2953739

Chalhoub, G., Kraemer, M. J., & Flechais, I. (2024). Useful shortcuts: Using design heuristics for consent and permission in smart home devices. *International Journal of Human-Computer Studies*, *182*, 103177. https://doi.org/10.1016/j.ijhcs.2023.103177

Chesbrough, H. (2003). *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Harvard Business School Press.

Cila, N., Smit, I., Giaccardi, E., & Kröse, B. (2017). Products as Agents: Metaphors for Designing the Products of the IoT Age. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17*, 448–459. https://doi.org/10.1145/3025453.3025797

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, *34*(1), 59–80. https://doi.org/10.1177/0268396218815559

Coiduras-Sanagustín, A., Manchado-Pérez, E., & García-Hernández, C. (2024). Understanding perspectives for product design on personal data privacy in internet of things (IoT): A systematic literature review (SLR). *Heliyon*, *10*(9), e30357. https://doi.org/10.1016/j.heliyon.2024.e30357

Costanza-Chock, S. (2020). *Design Justice: Community-Led Practices to Build the Worlds We Need*. The MIT Press.

Cranor, L. F., & Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems That People Can Use*. https://books.google.es/books?hl=en&lr=&id=mls7BB_ThMoC&oi=fnd&pg=PR5&dq=Garfinkel+%26+Cranor,+2005&ots=dc6Yt2Ewsv&sig=IHXTGKrZ8fOM5yeAIV7r1Xnmb34&redir_esc=y#v=onepage&q&f=false

Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L. F., & Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.*, *28*(6), 43:1-43:50. https://doi.org/10.1145/3469845

Dix, A., Finlay, J., & Abowd, G. (2004). *Human-computer Interaction*. Pearson Education.

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy Expectations and Preferences in an IoT World. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 399–412.

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)* (Regulation 2016/679; Official Journal of the European Union, pp. 1–88). Publications Office of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Frayling, C. (1993). Research in Art and Design. *Royal College of Art Research Papers*, *1*(1), 1–5.

Friedman, B., Kahn, P. H., & Borning, A. (2002). *Value Sensitive Design: Theory and Methods* (Technical Report 02–12). University of Washington. https://faculty.washington.edu/pkahn/articles/value-sensitive-design-theory-methods.pdf

Giaccardi, E., & Redström, J. (2020). Technology and More-Than-Human Design. *Design Issues*, *36*(4), 33–44. https://doi.org/10.1162/desi_a_00612

Greenleaf, G. (2014). *Global Data Privacy Laws 2014: 99 Countries, with European Laws Now a Minority*. (125), 14–18.

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering Privacy by Design. *Computers, Privacy & Data Protection*, *14*(3), 25–46.

Hernández-Ramírez, R. (2019). On false augmented agency and what surveillance capitalism and user-centered design have to do with it. *Journal of Science and Technology of the Arts*, 18-27 Páginas. https://doi.org/10.7559/CITARJ.V11I2.667

Iachello, G., & Hong, J. (2007). End-User Privacy in Human-Computer Interaction. *Foundations and Trends® in Human-Computer Interaction*, *1*(1), 1–137. https://doi.org/10.1561/1100000004

International Organization for Standardization. (2023). *ISO 31700:2023 Consumer Protection—Privacy by Design for Consumer Goods and Services* (Standard ISO 31700:2023). International Organization for Standardization. https://www.iso.org/standard/84977.html

 doi:10.20944/preprints202603.1128.v1

Kim, S., & Jung, Y. (2023). Development of Semantic Differential Scales for Artificial Intelligence Agents. *International Journal of Social Robotics*, *15*(7), 1155–1167. https://doi.org/10.1007/s12369-023-01010-3

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Langheinrich, M. (2001). Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In G. D. Abowd, B. Brumitt, & S. Shafer (Eds.), *Ubicomp 2001: Ubiquitous Computing* (Vol. 2201, pp. 273–291). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45427-6_23

Latour, B. (2005). *Reassembling the social: An introduction to Actor-Network-Theory*. Oxford University Press.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, *8*(6), 440–454. https://doi.org/10.1007/s00779-004-0304-9

Lupton, D. (2016). *The Quantified Self*. Polity Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 205395171454186. https://doi.org/10.1177/2053951714541861

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution that Will Transform how We Live, Work, and Think*. Houghton Mifflin Harcourt.

Mont, O. K. (2002). Clarifying the concept of product–service system. *Journal of Cleaner Production*, *10*(3), 237–245. https://doi.org/10.1016/S0959-6526(01)00039-7

Nielsen, J. (1993). *Usability Engineering*. Morgan Kaufmann.

Nielsen, J. (1994). Enhancing the explanatory power of usability heuristics. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 152–158. https://doi.org/10.1145/191666.191729

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Empowering People - CHI '90*, 249–256. https://doi.org/10.1145/97243.97281

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48.

Norman, D. A. (2013). *The design of everyday things* (Revised and Expanded). Basic Books.

Osgood, C. E. (1964). Semantic Differential Technique in the Comparative Study of Cultures. *American Anthropologist*, *66*(3), 171–200.

Parrilli, D. M. (2025). *Informational Privacy for Service Design: An Ethical Framework for Designing Privacy-Oriented Services* (Vol. 52). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-76926-9

Parrilli, D. M., & Hernández-Ramírez, R. (2022). Building a Privacy Oriented UI and UX Design: An Introduction to Its Foundations and Potential Developments. In N. Martins & D. Brandão (Eds.), *Advances in Design and Digital Communication II* (Vol. 19, pp. 16–30). Springer International Publishing. https://doi.org/10.1007/978-3-030-89735-2_2

PRISMA-P Group, Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., & Stewart, L. A. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews*, *4*(1), 1. https://doi.org/10.1186/2046-4053-4-1

Redström, J., & Wiltse, H. (2019). Changing Things. The Future of Objects in a Digital World. Bloomsbury Publishing.

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An Overview* [White Paper]. Internet Society. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

Rowland, C., Goodman, E., Charlier, M., Light, A., & Lui, A. (2015). *Designing Connected Products: UX for the Consumer Internet of Things*. O'Reilly Media, Inc.

Salgado, A. D. L. (2022). *Six Privacy and Usability Heuristics: From grounded models to validated new heuristics of usable privacy* [Doutorado em Ciências de Computação e Matemática Computacional, Universidade de São Paulo]. https://doi.org/10.11606/T.55.2022.tde-02062022-142408

Sayes, E. (2014). Actor–Network Theory and methodology: Just what does it mean to say that nonhumans have agency? *Social Studies of Science*, *44*(1), 134–149. https://doi.org/10.1177/0306312713511867

 doi:10.20944/preprints202603.1128.v1

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A Design Space for Effective Privacy Notices. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (1st ed., pp. 365–393). Cambridge University Press. https://doi.org/10.1017/9781316831960.021

Sharp, H., Preece, J., & Rogers, Y. (2019). *Interaction Design: Beyond Human-Computer Interaction* (5th ed.). Wiley.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. https://doi.org/10.2307/40041279

Solove, D. J. (2009). *Understanding privacy* (First Harvard University Press paperback edition). Harvard University Press.

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. University of Chicago Press.

VERBI Software. (2023). *MAXQDA 2024* [Computer software].

West, J., & Chesbrough, W. V. H. (2006). Open Innovation: A Research Agenda. In H. Chesbrough, W. Vanhaverbeke, & J. West (Eds.), *Open Innovation* (pp. 285–308). Oxford University Press. https://doi.org/10.1093/oso/9780199290727.003.0014

Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Law Review*, *25*(1), 166.

Zeng, E., Mare, S., & Roesner, F. (2017). End User Security & Privacy Concerns with Smart Homes. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security*, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Zimmerman, J., Forlizzi, J., & Evenson, S. (2007). Research through design as a method for interaction design research in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '07*, 493–502. https://doi.org/10.1145/1240624.1240704

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.