Metaphors as Scaffolds: Spatial, Relational, and Embodied Thinking for Youth Usable Privacy Design

JaeWon Kim
Information School
University of Washington
Seattle, Washington, USA
jaewonk@uw.edu

Alexis Hiniker
Information School
University of Washington
Seattle, Washington, USA
alexisr@uw.edu

Abstract

Drawing on observations from three prior studies with youth aged 13–24, we examine how metaphor shapes the way young people reason about privacy and imagine privacy designs beyond settings panels. *Spatial* metaphors made complex permission structures feel like movement through rooms and the placing of objects within them. *Embodied* metaphors gave youth language for shared norms around presence, access, and intrusion. *Fantastical* metaphors turned privacy work into something playful and discoverable, prompting more generative and granular design ideas. *Relational* metaphors, however, exposed the same mechanism's downside: when a system feels like a loyal companion while data passes through an institution, youth may disclose more than they otherwise would. This provocation does not argue that some metaphors are good and others bad. It argues that metaphors meaningfully scaffold both the design process and the user experience of usable privacy, and that choosing one is an ethical decision about which norms a privacy interface makes easy to see, imagine, and act on.

CCS Concepts

• **Human-centered computing → Collaborative and social computing**.

Keywords

usable privacy, youth, metaphor, social media, design, embodied cognition

ACM Reference Format:
JaeWon Kim and Alexis Hiniker. 2026. Metaphors as Scaffolds: Spatial, Relational, and Embodied Thinking for Youth Usable Privacy Design. In *Designing Interactive Systems Conference (DIS Companion '26), June 13–17, 2026, Singapore, Singapore.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3802974.3809449

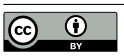
1 Introduction

Privacy interfaces are full of metaphors. People "manage" privacy through "settings," "controls," "permissions," and "walls." These words sound neutral, but they teach users to understand privacy in a particular way: as something an individual should configure correctly through an interface. For adults already fluent in privacy logic based in access control, the framing is workable, if cumbersome. For youth, whose privacy is relational and norm-dependent [2, 13, 16], it fits poorly. Adolescents do not navigate privacy only by choosing among toggles. They read social cues, calibrate trust, and co-manage boundaries with peers in real time [9, 17]. Administrative controls give them little help with that work.

The mismatch is not only a usability problem; it is also a design imagination problem. When privacy is rendered as a list of toggles and dropdowns, better privacy tends to mean a clearer list, a shorter consent flow, or a more precise toggle. Metaphors open up other ways of thinking. They let designers and users ask what privacy might look like as a room, a door, a secret handshake, a map, a status light, or a relationship.

That generative power is why metaphor choice carries ethical weight. The words a privacy interface uses suggest what kind of situation the user is in, what norms apply, and what response makes sense. Metaphors also expand what counts as the design space in the first place: a room invites thinking about thresholds and guests, a handshake invites thinking about mutual recognition, a status light invites thinking about ambient presence. Each opens a different set of interface possibilities that a list of toggles does not make visible. Privacy concepts are already metaphorical, whether designers intend them to be or not. The design question is which metaphors a system uses, what reasoning those metaphors support, what interface possibilities they make imaginable, and whose interests they serve.

This provocation revisits three prior studies with youth aged 13–24 [6, 8, 9]. None of the studies was designed to investigate metaphor. The pattern surfaced across them: different framings repeatedly changed what participants found easy to reason about or design. We organize the pattern into four cases. *Spatial* metaphors helped youth handle privacy complexity by mapping it onto familiar ideas of rooms, paths, and presence. *Embodied* metaphors helped peers describe shared norms, such as when entering a space or taking up attention feels appropriate. *Fantastical* metaphors made privacy management playful enough to invite more ambitious designs. The fourth case complicates the positive account: *relational* metaphors can lead youth past boundaries they would otherwise maintain, especially when the felt relationship does not match the underlying data relationship. Across these projects, metaphors shaped what counted as a privacy decision in the first place. We argue that metaphor selection deserves treatment as an early design decision about which privacy norms become available to young users and which possibilities designers learn to imagine.



DIS Companion '26, Singapore, Singapore

ACM ISBN 979-8-4007-2632-3/26/06
https://doi.org/10.1145/3802974.3809449

2 Background

2.1 Privacy as Networked Boundary Regulation

HCI has long treated privacy not as individual secrecy but as the ongoing regulation of social boundaries [1, 12, 13]. Communication Privacy Management (CPM) [13] frames disclosure as the co-management of information through implicit privacy rules. When those rules are shared, boundary regulation proceeds smoothly; when they are not, "boundary turbulence" follows. Networked environments make this work harder.

Hyperpersonal communication [15] amplifies social signals under reduced cues, and boyd's ethnography [2] shows teens negotiating privacy under conditions of persistence, searchability, and invisible audiences. Other work [7, 16] finds that teens often go along with whatever a platform's dominant practices reward, even when those practices conflict with their stated preferences, because the social cost of deviating is high and the rules are hard to name.

2.2 Metaphor as a Design Surface

Lakoff and Johnson's theory of conceptual metaphor [10] argues that people reason about abstract concepts by mapping from concrete, embodied experience. The choice of metaphor changes which inferences feel obvious. A privacy "wall" can be breached but is hard to negotiate with. A privacy "dance" suggests mutual adjustment. A privacy "room" suggests entry, presence, and different expectations in different places.

Most privacy interfaces default to an administrative framing: settings, controls, permissions, and consent. This framing assumes users can translate messy social situations into abstract access rules. Nissenbaum's contextual integrity framework [11] argues that information flows are appropriate when they fit the norms of their context, and prior work shows how platform framing can shape which norms feel applicable in the first place [4].

3 Background on the Studies

This provocation grew out of three prior studies with youth aged 13–24. We briefly describe each below to give readers the context needed to follow the cases.

Project H: Social Media at Hogwarts. This study [6] used co-design interviews with the Fictional Inquiry (FI) method [3] with 23 participants aged 15–24. Participants imagined how students at a wizarding school might connect with friends using any magical powers they could envision. The fictional frame served as a defamiliarization strategy: avoiding the term "social media" allowed participants to reason from felt experience rather than from preconceived ideas about mainstream platforms. The protocol included a segment in which participants imagined a house-elf character (Dobby) as a personal assistant within their envisioned social space. Participants are denoted H01–H23.

Project D: Discord as Virtual Third Place. This study [8] used semi-structured interviews with 25 participants aged 15–24, examining how Discord's design supports relationship formation and a sense of place. Discord was selected because participants in earlier studies in our group had repeatedly named it as their primary site for friendship building without prompting. Participants in Project D were not cued with spatial language or the concept of "third places"; place-based analogies emerged on their own. Participants are denoted D01–D25.

Project T: Trust-Enabled Privacy. This study [9] used a three-part design (entry interviews, diary study, co-design interviews) with 19 teens aged 13–18, examining barriers to meaningful self-disclosure on broadcast-centered platforms such as Instagram. A recurring theme was the problem of involuntary, public-feeling exposure: participants described how posting inserted their content unbidden into other users' feeds, which felt akin to occupying public space without permission. Participants are denoted T01–T19.

4 Case 1: Spatial Metaphors Make Complex Privacy Easier to Navigate

Discord is visually two-dimensional, but it supports unusually granular access control: nested servers, channels, role-based permissions, voice rooms with visible occupants, and ad hoc invitations. Participants in Project D handled this complexity with little of the frustration youth often describe around privacy settings, and they explained why in spatial terms. Without prompting, they described Discord as a set of places: D11 called it a "town square," D20 a "concert hall" with themed rooms, D07 a "café," and D24 an organized "house" with distinct sections.

Participants used these analogies to decide where to participate, judge appropriate behavior, and interpret other people's intentions. Discord's channel architecture maps permission complexity onto the familiar logic of spatial partitioning: different rooms for different purposes, visible presence, bounded membership, and expectations about who belongs where. The mapping does some of the privacy work that other platforms offload onto explicit settings. Knowing which channel to speak in, who is present in a voice room, and whose server one is visiting are spatial questions before they are technical permission questions.

The spatial framing does not remove complexity so much as route it through intuitions people already use without instruction [10]. The point matters for youth in particular because complex settings often become something to avoid rather than something to use [9]. The design implication is not that every privacy interface should look like a room, but that spatial organization can make complicated boundary rules understandable without requiring users to hold the whole access-control model in their heads.

5 Case 2: Embodied Metaphors Help People Name Shared Boundary Norms

Embodied metaphors help people coordinate norms with one another. They give users plain language for access, presence, intrusion, and consideration—the kinds of jointly held privacy rules central to CPM [13] but often left unnamed by platform settings.

In Project H, participants asked to imagine a Hogwarts-style social space generated access norms that mapped onto everyday embodied experience. H03 described public areas like "the downstairs area," "guest bedroom," or "game room" as spaces where people could "just come in," while a private bedroom required "extra consent" because it was a "safe space." H13 proposed an intermediate "waiting room" for sharing "semi-personal things" before granting further access. H22 expected spatial norms to transfer directly: "Why would you want to go into my virtual bedroom when I'm

not even home? If I wouldn't do it in real life, I probably wouldn't want to do it online either." Participants designed independently but arrived at a compatible sense of what different spaces allowed. The metaphor of entering and occupying space made boundary expectations legible without requiring explicit rules.

Project T offers a second example. Teens on broadcast platforms described posting as taking up space in other people's feeds. They worried about "clogging" (T16) or "spamming" (T03, T13), and T09 described regret after "shar[ing] a TON of reels today on my close friends and public for some reason :crying-face:". On the receiving side, T12 said "If I'm following 100 people and they're all sharing four times a day, then that's 400 things I have to click through." Posting was not only self-expression; it was also a use of shared attention. The implicit norm was considerate occupancy.

This language made a privacy problem socially intelligible. Overposting did not only expose the poster; it imposed on others. Yet the platform gave participants no design surface for naming public, personal, or shared space. Participants therefore proposed self-contained alternatives, including "a little status update" or "a red dot" on profiles, that would let them share without pushing content into others' feeds. The stakes here are youth-specific: prior work documents that teens may hesitate to enact privacy preferences when doing so risks making them look "uptight" [7]. Embodied metaphors help by turning private preference into a shared norm: not "I am being difficult," but "we should have a less intrusive way to occupy each other's attention."

6 Case 3: Fantastical Metaphors Make Privacy Design More Generative

Digital environments are not bound by physical law. Designers can invent doors that appear only for certain people, maps that reveal presence selectively, or spaces that open through shared rituals. Privacy interfaces rarely use that freedom, defaulting instead to lists of toggles that are tedious to maintain and easy to abandon [5, 7]. Project H suggests that fantastical metaphors help youth imagine privacy mechanisms richer than what toggle lists can express, because they turn privacy work into something playful and discoverable.

Participants in Project H repeatedly invented privacy mechanisms that were both game-like and socially meaningful. H11 imagined controlling space access through "secret knock" gestures or hidden objects revealing "secret passages" for trusted friends. H21 proposed "secret handshakes" shared among friend groups. Drawing on the Marauder's Map, H02 imagined privacy controls activated by "spells" that unlocked spaces when correctly summoned. H05 compared these mechanisms to "little Easter eggs," contrasting them with mainstream social media's "wall of settings" that often felt confusing.

These designs were often more granular than existing privacy controls, not less. What changed was the feel of the work. A wall of toggles is a chore one completes in order to be safe, whereas a secret handshake among friends is something one might want to maintain. The distinction has practical bite because nuanced self-presentation across audiences requires ongoing adjustment. If every adjustment feels like administrative labor, youth tend to avoid it. If the same adjustment is folded into play, discovery, or friendship, it becomes part of the interaction rather than a cost imposed on it. Metaphor, then, is a method for privacy design and not merely a style for explaining a finished interface.

7 Case 4: Relational Metaphors Can Misdirect Trust

Relational metaphors activate trust-based reasoning. When the felt relationship matches the actual data relationship, they support disclosure and care. When the two diverge, the metaphor leads users to apply interpersonal norms to an institutional system.

In Project H, participants imagined a house-elf character (Dobby), drawn from *Harry Potter*, where the character is known for unwavering loyalty, as a personal assistant. Participants developed trust in the imagined assistant quickly, often within minutes. H03 renegotiated Dobby's role from servant to companion: "I scratch the idea that he's a maid. He's not a maid… He's like a roommate… He can see everything that I can see." H04 described Dobby as someone they would confide in about "problems that I couldn't discuss with anyone… in the real, like, solid world." The relational frame made disclosure feel safe, not because participants had evaluated the privacy implications, but because the metaphor placed them in a context where disclosure to a trusted companion made sense.

The picture shifted when the interviewer introduced the "House Elf Association," a narrative device for institutional data collection. H02, who had initially granted Dobby full access ("Dobby would have access to everything… since they're super loyal"), immediately recalibrated: "I'd kind of be… concerned… but not my vaults… from when I was younger… something I really don't want judged." The companion metaphor had set up friendship norms: loyalty, care, and broad access. The institutional prompt moved the situation into a different context with different expectations.

In Nissenbaum's terms [11], the companion metaphor created a contextual-integrity problem: it made one context feel present while the actual information flow belonged to another. The risk is acute for AI companion products such as Character.ai and Replika, where relational framing dresses up institutional data collection as interpersonal exchange [14, 18, 19]. H04's willingness to share with Dobby "problems that I couldn't discuss with anyone… in the real, like, solid world" captures, at small scale, the privacy risk posed by relational AI. The mechanism that helped participants reason productively in the earlier cases becomes a tool for extracting disclosure when relational warmth is deployed by a system whose incentives diverge from the user's.

8 Discussion

Across these cases, metaphors helped youth reason about privacy in ways that settings panels often do not, while also showing how a compelling frame can make the wrong norms feel applicable. The synthesis is interpretive. The cases were chosen because they make the contrast visible, not because they represent all youth or all privacy designs. Our 13–24-year-old participants were U.S.-based and familiar with *Harry Potter* and gaming, which likely shaped how spatial and fantastical framings transferred. Settings-based controls remain useful in some contexts, including legally required consent flows. The argument is not that administrative controls should disappear. It is that they should not be the default model for privacy

problems that are social, relational, and context-dependent. Future studies designed around metaphor from the outset, for instance by comparing identical privacy structures under different framings and tracing effects on actual disclosure, would help test the empirical claims raised here.

The central design implication is that metaphors should be evaluated on two questions. First, what do they help people imagine? A metaphor expands the design space, as the spatial, embodied, and fantastical cases show. Second, what do they make harder to see? A metaphor also hides institutional actors, data movement, and power asymmetries, as the relational case shows.

What surfaces across these cases is not a privacy literacy gap. Youth reason about disclosure with strong attention to relationship, context, and social norms. What platforms often demand is fluency in the place where that reasoning works least well: abstract administration. Rather than teaching young people to translate relational intuitions into checkbox configurations, designers and policymakers might build environments where those intuitions guide privacy decisions directly. Metaphor choice is not neutral. It deserves treatment as an early, explicit design decision about how a privacy interface helps young users reason, what it helps designers imagine, and what it may hide.

Acknowledgments

JaeWon Kim would like to acknowledge the CERES Network, University of Washington Global Innovation Funds (GIF), and Student Technology Funds (STF), which provided support for this work. This work was also funded in part by the Paul G. Allen School of Computer Science & Engineering Endowed Fund for Excellence and a gift from Google. Alexis Hiniker is a special government employee for the Federal Trade Commission. The content expressed in this manuscript does not reflect the views of the Commission or any of the Commissioners.

References

[1] Irwin Altman and Dalmas A Taylor. 1973. Social penetration: The development of interpersonal relationships. 212 (1973).

[2] danah boyd. 2014. *It's Complicated: The Social Lives of Networked Teens.* Yale University Press.

[3] Christian Dindler and Ole Sejer Iversen. 2007. Fictional Inquiry—design collaboration in a shared narrative space. *CoDesign* 3, 4 (December 2007), 213–234. doi:10.1080/15710880701500187

[4] Meira Gilbert, Miranda Wei, and Lindah Kotut. 2025. "TikTok, Do Your Thing": User Reactions to Social Surveillance in the Public Sphere. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security* (Seattle, WA, USA) *(SOUPS '25)*. USENIX Association, USA, Article 18, 18 pages.

[5] Jane Im, Ruiyi Wang, Weikun Lyu, Nick Cook, Hana Habib, Lorrie Faith Cranor, Nikola Banovic, and Florian Schaub. 2023. Less is Not More: Improving Findability and Actionability of Privacy Controls for Online Behavioral Advertising. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23, Article 661)*. Association for Computing Machinery, New York, NY, USA, 1–33. doi:10.1145/3544548.3580773

[6] JaeWon Kim, Hyunsung Cho, Fannie Liu, and Alexis Hiniker. 2026. Social Media Should Feel Like Minecraft, Not Instagram: Youth Visions for Meaningful Social Connections through Fictional Inquiry. arXiv:2502.06696 [cs.HC] https://arxiv.org/abs/2502.06696

[7] JaeWon Kim, Soobin Cho, Robert Wolfe, Jishnu Hari Nair, and Alexis Hiniker. 2025. Privacy as Social Norm: Systematically Reducing Dysfunctional Privacy Concerns on Social Media. *Proc. ACM Hum.-Comput. Interact.* 9, 2, Article CSCW151 (May 2025), 39 pages. doi:10.1145/3711049

[8] JaeWon Kim, Thea Klein-Balajee, Ryan M. Kelly, and Alexis Hiniker. 2025. Discord's Design Encourages "Third Place" Social Media Experiences. arXiv:2501.09951 [cs.HC] https://arxiv.org/abs/2501.09951

[9] JaeWon Kim, Robert Wolfe, Ramya Bhagirathi Subramanian, Mei-Hsuan Lee, Jessica Colnago, and Alexis Hiniker. 2025. Trust-enabled privacy: social media designs to support adolescent user boundary regulation. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security* (Seattle, WA, USA) *(SOUPS '25)*. USENIX Association, USA, Article 27, 20 pages.

[10] George Lakoff and Mark Johnson. 1980. *Metaphors We Live By.* University of Chicago Press.

[11] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (February 2004), 119–157.

[12] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA. doi:10.1145/642611.642635

[13] Sandra Petronio. 2002. *Boundaries of Privacy: Dialectics of Disclosure.* SUNY Press.

[14] Jenny Radesky, Marie A Bragg, and Alexis Hiniker. [n. d.]. Risks and Consequences of Children's Use of Social AI—A Framework. *JAMA pediatrics* ([n. d.]).

[15] Joseph B. Walther. 1996. Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction. *Communication Research* 23, 1 (1996), 3–43.

[16] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, 51–69.

[17] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Austin, Texas, USA). *GROUP ACM SIGCHI Int. Conf. Support. Group Work*, 609–618. doi:10.1145/2207676.2207761

[18] Yaman Yu, Yiren Liu, Jacky Zhang, Yun Huang, and Yang Wang. 2025. Youth-Centered GenAI Risks (YAIR): a taxonomy of generative AI risks from empirical data. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security* (Seattle, WA, USA) *(SOUPS '25)*. USENIX Association, USA, Article 9, 17 pages.

[19] Yaman Yu, Tanusree Sharma, Melinda Hu, Justin Wang, and Yang Wang. 2025. Exploring Parent-Child Perceptions on Safety in Generative AI: Concerns, Mitigation Strategies, and Design Implications . In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 2735–2752. doi:10.1109/SP61157.2025.00090