# A design space for privacy negotiation

Yi-Shyuan Chiang
*University of Illinois Urbana-Champaign*

Pia Robinson
*University of Illinois Urbana-Champaign*

Camille Cobb
*University of Illinois Urbana-Champaign*

Weijia He
*University of Southampton*

## Abstract

Smart home devices are becoming more common in American households. Past research focuses on privacy notices and choice mechanisms for smart home devices. Current notice-and-choice mechanisms do not account for whether individuals can make informed decisions about their privacy preferences. Privacy negotiations allow individuals to negotiate their privacy preferences and make informed decisions. A design space for privacy negotiations to be present as well allows data subjects to have greater say in their privacy preferences and more control over their data and information. In this poster, we present a preliminary design space for privacy negotiations and discuss future plans.

## 1 Introduction

Over 45% of American households have at least one smart home device [5]. Privacy concerns about smart devices and their ubiquitous, long-term data-collection capabilities have become prevalent [14, 15, 25, 30].

Prior work has focused on the "notice and choice" mechanisms, e.g., informing and then obtaining privacy choices [12, 20, 21, 24, 26]. Notice and choice mechanisms assume that once individuals have information, they can make informed decisions that best reflect their privacy preferences, which may *not* be the reality. Sloan and Warner argued that notice and choice are merely passive acquiescence rather than informed consent due to the insufficient information that can fit into a readable notice [23]. Social factors, such as employment and social positions, can affect how truthful and protective these privacy decisions are [1, 2, 7, 8]. For example, tenants might feel uncomfortable to voice privacy preferences *in situ* [28].

Therefore, to give individuals more agency in managing their privacy rights, much more should happen between a notice and a choice. One common example is privacy negotiation. It allows data subjects to propose their preferred settings rather than accept whatever is offered [3, 28, 31].

Past design spaces have focused only on privacy notices and choices [12, 21], sharing design dimensions, e.g., type, timing, channel, and modality. **We argue that privacy negotiation is an emerging part of privacy communication and is in need of a design space.** Design spaces allow stakeholders to systematically generate, iterate, and evaluate current and future designs for privacy negotiation. They also provide stakeholders with language to communicate the different designs. The intended contribution of this work is as follows: a design space for privacy negotiation and demonstrations of how to utilize the design space.

## 2 Method

We adopted the QOC (Questions, Options, Criteria) Framework to perform design space analysis [16, 19]. The QOC framework has previously been used by Schaub et al. to analyze design spaces for privacy notices [21]. The QOC framework starts with guiding questions to guide the ideation of the options. We use the following question to ground the ideation: What are the design space for privacy negotiations? We then brainstorm design options with reference and inspiration components surfaced from prior privacy notice and choice work [12, 21]. With the set of options, the research team then applies a set of criteria to examine the options.

## 3 Preliminary results

We referred to previous privacy design spaces [12, 21] and propose the following design space for privacy negotiation (See Figure 1).


*USENIX Symposium on Usable Privacy and Security (SOUPS)* 2026.
August 23–26, 2026, Hannover, Germany.

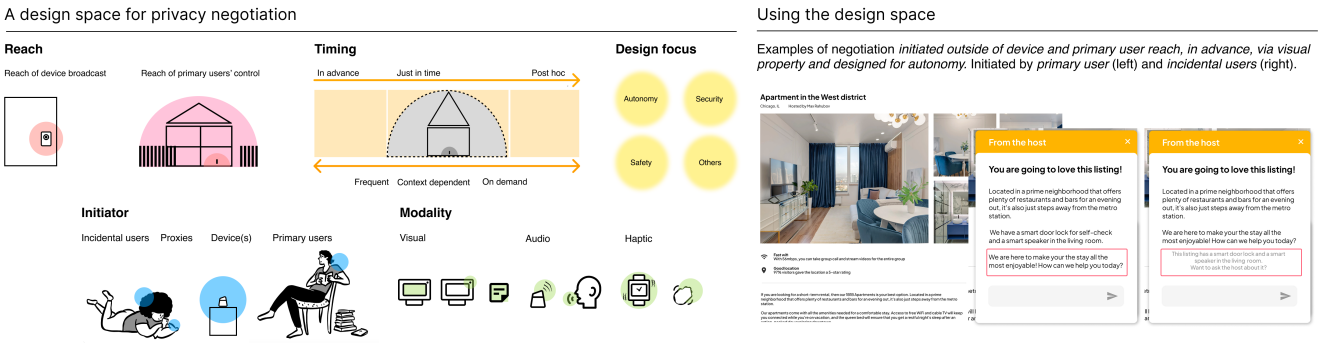


Figure 1: **A design space for privacy negotiation & examples of using the design space** We propose the 5 dimensions for privacy negotiation: Reach, Timing, Design focus, Initiator, Modality.

**Design focus:** Negotiations can center around different focuses. The common design focuses from past research are autonomy, security, and safety [9, 13]. The design of the negotiation process can vary depending on the desired focus. For example, if individuals are negotiating for autonomy, then the process should focus on discussing individuals' control. If the focus is data subjects' security, the negotiation process might focus more on developing security protocols.

**Reach:** The physical presence of the devices and stakeholders can affect negotiation, e.g., how and where negotiations take place. Past research has found that people prefer to negotiate *ex ante* [3]. This means devices' built-in features might not be helpful because their broadcasting and data collection capabilities are limited to their physical reach. For example, smart speakers' built-in microphones can only capture sound up to 10 to 30 ft. On the other hand, the reach of device owners and primary users includes not only the devices but also their surroundings and the property as a whole. They have chances to put up signs or verbally inform the guests when they arrive on the premises of the property, but are still outside of the devices' reach [11].

**Timing:** Negotiation can happen at different timings and at different frequencies. It can happen in advance of the data collection or when individuals are just about to enter the reach of devices. Negotiation can also happen after the data collection on how the collected data should be handled and the preferred future collection practices [12]. Negotiation can also occur frequently throughout the data collection: individuals can negotiate on demand, in context, or at preset frequencies [12, 21].

**Initiator:** Negotiation can be initiated by various entities. Device owners are perceived to have the most control over the devices and therefore should be responsible for data collection [10]. Incidental users could also initiate the negotiation; however, they might feel less inclined to do so to avoid social awkwardness or retaliation [4, 31]. Devices could also initiate interactions with built-in features, such as privacy assistants that facilitate negotiation when they register unfamiliar voices [26]. Privacy assistants could also initiate negotiations on behalf of their owners, either based on user-specified rules or on their behaviors [17, 18, 22, 27].

**Modality:** Negotiation can be initiated and conducted through different modalities. Digital screens, as a visual modality, enable people to easily interact and indicate their negotiation settings [24, 29]. Audio, such as voice assistants, can easily facilitate or even initiation negotiation that take place in verbal communication [6, 24]. Haptic feedback can also initiate or serve as a reminder to initiate privacy negotiation.

## 4 Use cases

The design space allows us to **generate** design ideas by combining different design space dimensions. It will also allow us to **evaluate** designs from previous literature, **map** design gaps, and **iterate** on existing designs. For example, one design combination could be negotiation *initiated outside of device reach and primary user reach, in advance, by primary users, via visual property and designed for security*. We envision this design for short-term rental scenarios in Figure 1. Texting interfaces could come with messaging prompts that either encourage property owners to initiate the conversion or introduce the negotiation by default.

## 5 Conclusion & future plan

We present a preliminary design space for privacy negotiation in this poster, spanning design focus, reach, timing, initiator, and modality. We plan to further ideate on the design space, conduct more in-depth case studies on how existing systems fit within it, and discuss how stakeholders can work with it.

## References


[1] Wael Albayaydh and Ivan Flechais. Exploring bystanders' privacy concerns with smart homes in jordan. In *CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2022.

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

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

[4] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. Exploring the privacy concerns of bystanders in smart homes from the perspectives of both owners and bystanders. *Proceedings on Privacy Enhancing Technologies*, 2022.

[5] Fiber Broadband Association. The smart home in 2025: Outlook and opportunities, 2025. https://fiberbroadband.org/2025/01/29/the-smart-home-in-2025-outlook-and-opportunities/ [Accessed: 2026.2.25].

[6] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. Para: Privacy management and control in emerging iot ecosystems using augmented reality. In *Proceedings of the 2021 international conference on multimodal interaction*, pages 478–486, 2021.

[7] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. {Bystanders'} privacy: the perspectives of nannies on smart home surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[8] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. Smart home bystanders: Further complexifying a complex context. In *Proceedings of CI Symposium*, 2019.

[9] Yi-Shyuan Chiang and Camille Cobb. Do we have a shared understanding of consent? In *Moving Beyond Clicks: Rethinking Consent and User Control in the Age of AI (CHI'26 Workshop)*, 2026.

[10] Yi-Shyuan Chiang, Omar Khan, Adam Bates, and Camille Cobb. More than just informed: The importance of consent facets in smart homes. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–21, 2024.

[11] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "i would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 2021.

[12] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[13] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. Sok: Context sensing for access control in the adversarial home iot. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 37–53. IEEE Computer Society, 2021.

[14] Alex Hern. Amazon staff listen to customers' alexa recordings, report says, 2019. https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says [Accessed: 2026.2.25].

[15] Dan Latu. Airbnb host secretly recorded over 2,000 images of guests with his security camera, authorities said, 2024. https://www.businessinsider.com/texas-airbnb-host-hidden-security-camera-recorded-guests-2024-7 [Accessed: 2026.2.17].

[16] Allan MacLean, Richard M Young, Victoria ME Bellotti, and Thomas P Moran. Questions, options, and criteria: Elements of design space analysis. In *Design rationale*, pages 53–105. CRC Press, 2020.

[17] Nathan Malkin, David Wagner, and Serge Egelman. Runtime permissions for privacy in proactive intelligent assistants. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 633–651, 2022.

[18] Karola Marky, Alina Stöver, Sarah Prange, Kira Bleck, Paul Gerber, Verena Zimmermann, Florian Müller, Florian Alt, and Max Mühlhäuser. Decide yourself or delegate-user preferences regarding the autonomy of personal privacy assistants in private iot-equipped environments. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2024.

[19] Diane McKerlie and Allan MacLean. Reasoning with design rationale: practical experience with design space analysis. *Design Studies*, 15(2):214–226, 1994.

[20] Bayan Al Muhander, Omer Rana, and Charith Perera. Privify: Designing tangible interfaces for configuring iot privacy preferences. *arXiv preprint arXiv:2406.05459*, 2024.

[21] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*, pages 1–17, 2015.

[22] Daniel D Slate, Chaoran Chen, Yaxing Yao, and Toby Jia-Jun Li. Iterative contextual consent: Ai-enabled data privacy contracts. In *Proceedings of the 2025 Workshop on Human-Centered AI Privacy and Security*, pages 84–91, 2025.

[23] Robert H. Sloan and Richard Warner. Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal of High Technology Law*, 14(2):370–414, 2014.

[24] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I Hong. I'm all eyes and ears: Exploring effective locators for privacy awareness in iot scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[25] Akim Powell Tabitha Bland. Guest allegedly finds hidden cameras inside bathroom outlets of airbnb, police say, 2025. https://www.weau.com/2025/08/04/guest-allegedly-finds-hidden-cameras-inside-bathroom-outlets-airbnb-police-say/ [Accessed: 2026.2.25].

[26] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "it would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2022.

[27] Onuralp Ulusoy and Pinar Yolum. Panola: A personal assistant for supporting users in preserving privacy. *ACM Transactions on Internet Technology (TOIT)*, 22(1):1–32, 2021.

[28] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. Exploring tenants' preferences of privacy negotiation in airbnb. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 535–551, 2023.

[29] Maximiliane Windl, Philipp Thalhammer, David Müller, Albrecht Schmidt, and Sebastian S Feger. Privacyhub: A functional tangible and digital ecosystem for interoperable smart home privacy awareness and control. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2025.

[30] Soo Youn. Alexa is always listening — and so are amazon workers, 2019. https://abcnews.com/Technology/alexa-listening-amazon-workers/story?id=62331191 [Accessed: 2026.2.25].

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