Let's *talk* about privacy

Sarah Pearman

May 9, 2022

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee:
Lorrie Faith Cranor, Chair
Alessandro Acquisti
Eleanor Birrell
Nicolas Christin

Copyright © 2022 Sarah Pearman

Abstract

While many studies have shown that the notice and choice paradigm constitutes a significant burden and challenge for users, and while research has been done to explore best practices to make this situation a bit better, the overall status quo is still quite poor. This problem will only grow as more devices become internet-connected and as these devices become more diverse in functionality and interaction type. In this thesis, I will offer evidence that our current GUI-focused paradigms for notice and choice research are not keeping up with emerging technologies, propose additional ways of thinking about privacy choices, and test some approaches that could be more fitting, particularly in the context of conversational interfaces.

I will first describe a body of collaborative work from the past few years in which I have explored how current privacy interfaces and tools do and do not meet users' needs. This will include discussing recent work on websites' opt-out and data deletion choices as well as advertising controls on Facebook.

Next, I will describe a three-phase case study in which I iteratively redesigned and evaluated the consent flow for a chatbot being developed for a large U.S. health insurance company's online platform. Ultimately, simplifying the interface and language of the consent flow did help to improve the overall user experience and usability, and users did understand important points better with the redesigned versions *if* they were instructed to revisit them a second time. However, the redesigns made little to no detectable difference in what users understood when going through the flow in a natural way with another non-privacy task as the main focus, supporting the idea that the overall paradigm of presenting users with legal documents unrelated to their primary tasks is fundamentally dysfunctional.

The penultimate chapter will focus on a study in which I am comparing standard privacy policy disclosures to a more conversational approach in the context of signup and onboarding for a social media app. I created five interactive prototypes that vary in terms of (1) how much privacy information is presented on the main screen and (2) whether they present additional privacy information primarily via a standard data policy link or via an approach where participants can choose from a set of likely questions in a more conversational style. To test these, I am applying the evaluation framework proposed in Hana Habib's doctoral thesis [11], focusing on user needs, ability and effort, awareness, comprehension, and sentiment.

In the final portion of my thesis, I plan to build and test a voice user interface prototype that offers voice-based privacy interactions rather than the decoupled interactions that platforms like Alexa currently tend to offer. I will explore and report on any conflicts between best practices for privacy notice and choice and best practices for voice interface design that I encounter. I will then gather qualitative and quantitative data to compare this prototype to existing decoupled approaches, evaluating based on Habib's framework.

Contents

Chapter 1

Introduction

Ultimately, while a number of studies have demonstrated that understanding privacy disclosures and making privacy choices are significant burdens for users, and while research has been done to explore best practices to make this situation a bit better, the overall status quo is still quite poor. Privacy notices are notoriously long and time consuming to read [21], and they tend to be written in language that serves to ease the minds of company lawyers rather than helping the average user to Some studies show that shortening and simplifying disclosures may help users understand the choices available to them [9, 17], but others have shown little effect from simplifying such disclosures [3]. In addition to spending hundreds of hours per year reading legal documents to understand what they were agreeing to when signing up for and using services, to make choices such as opting out of data collection, a user often must spend a great deal of time and effort finding privacy options buried in difficult-to-discover menus.

The problems with the existing notice and choice paradigm will only be worsened with the increasing prevalence of emerging technologies that use types of interfaces that lend themselves poorly to presenting users with a long document to read on a screen. Our status quo wherein users are expected to visually read privacy disclosures and then make privacy choices using a GUI does not fit neatly with emerging technologies such as voice assistants or extended reality platforms.

In this thesis, I will offer evidence that our current GUI-focused paradigms for notice and choice research are not keeping up with emerging technologies, propose additional ways of thinking about privacy choices, and test some approaches that could be more fitting, particularly in the context of conversational interfaces.

I will first describe a body of collaborative work from the past few years in which I have explored how current privacy interfaces and tools do and do not meet users' needs. This will include discussing recent work on websites' opt-out and data deletion choices as well as advertising controls on Facebook.

In the next chapter, I will describe a three-phase case study in which I iteratively redesigned and evaluated the consent flow for a chatbot being developed for a large U.S. health insurance company's online platform. In this study, I first conducted a remote usability study to obtain qualitative data about usability and user understanding, and I used those findings as well as best practices to improve the design of the consent flow. I then compared the original version to redesigned versions in two online surveys. Ultimately, simplifying the interface and language

of the consent flow did help to improve the overall user experience and usability, and users did understand important points better with the redesigned versions *if* they were instructed to revisit them a second time. However, the redesigns made little to no detectable difference in what users understood when going through the flow in a natural way with another non-privacy task as the main focus, supporting the idea that the overall paradigm of presenting users with legal documents unrelated to their primary tasks is fundamentally dysfunctional.

The penultimate chapter will focus on a study that is in progress in spring 2022 in which I am comparing standard privacy policy disclosures to a more conversational approach, partially inspired by video games, in the context of signup and onboarding for a social media app. I created five interactive prototypes that vary in terms of (1) how much privacy information is presented on the main screen and (2) whether they present additional privacy information primarily via a standard data policy link or via an approach where participants can choose from a set of likely questions in a more conversational style. To test these, I am applying the evaluation framework proposed in Hana Habib's doctoral thesis [11], focusing on user needs, ability and effort, awareness, comprehension, and sentiment. I am currently conducting a remote user study with a task and semi-structured interview to obtain qualitative data about these prototypes, and I will later conduct an online survey via Prolific to gather quantitative data to compare the prototype versions and examine whether the more conversational versions of the prototype confer any advantages.

In the final portion of my thesis, I plan to build and test a voice user interface prototype that offers voice-based privacy interactions rather than the decoupled interactions that platforms like Alexa currently tend to offer to users who ask voice assistants about their privacy practices or options. I intend for this prototype to incorporate best practices for privacy notice and choice and for voice interface design. I will explore and report on any conflicts between best practices for privacy notice and choice and best practices for voice interface design that I encounter. I will then gather qualitative and quantitative data to compare this prototype to existing decoupled approaches. First, to iterate on a design to test, I will gather qualitative data about how users naturally discuss privacy in real-world conversations, as well as data about users' perceptions of and interactions with preliminary versions of the prototype. I will then compare the performance of a final prototype to an existing decoupled approach in a quantitative study and compare it to the current status quo for voice interface privacy interactions on metrics related to user needs, effort, awareness, comprehension, and sentiment.

Thesis statement

This thesis will highlight problems with current privacy notice and choice practices and demonstrate when and how conversational approaches to notice and choice may improve the experience for users (understanding of what they have consented to, satisfaction with their choices, and trust in the system).

Chapter 2

Background and related work

2.1 Notice and choice 1.0: The wall of text

Historically, we have relied on privacy policies and the like to provide technology users with a semblance of informed choice. We know, however, that someone who read all of the privacy notices for all of the products and services that they used could be expected to spend hundreds of hours per year on this task [21]. Unsurprisingly, less than a quarter of U.S. adults surveyed by Pew Research in 2019 reported that they always or often read privacy policies, and 36% reported *never* reading them [**?**].

One reason for this is certainly the length and complexity of these documents, and numerous researchers have explored methods of shortening and simplifying disclosures to help users efficiently grasp the most important details. Studies have suggested that approaches such as short-form policies and "privacy nutrition labels" can help users find and understand privacy information [9, 17]. In addition, a study on End User License Agreements (EULAs) found that users spent more time reviewing paraphrased EULAs than traditional long-form EULAs, and that paraphrased EULAs yielded more positive sentiments and higher comprehension [**?**]. However, in a study by Ben-Shahar and Chilton, policy simplifications had little to no effect on users' understanding or their consent choices. The authors of that study speculate that users may be entirely "numb" and "unmotivated to use privacy notices of any kind" [3].

2.2 Notice and choice 2.0: Better "best" practices

Researchers have established some best practices that might improve users' chances of actually understanding privacy disclosures and making informed decisions that match their intentions and values. In 2015, Schaub et al. reviewed the literature on privacy notice design and made a number of recommendations...

In the first study described in my thesis, I applied many of these best practices to the HIPAA authorization for a healthcare chatbot, including identifying and providing control over practices that might be unexpected, avoiding jargon, conducting user testing, and trying not to overwhelm users with multiple choices.

2.3 Notice and choice 3.0?: Conversational privacy as a potential tool for emerging technology contexts

There is a growing interest in the topic of "conversational privacy" as an alternative to traditional notice and choice paradigms, which are known to have low usability. Conversational privacy could end up being especially beneficial in the context of conversational user interfaces (CUIs), since it could offer notice and choice mechanisms native to the interface in question. As of 2022, common voice assistant platforms such as Alexa, Siri, and Google Home have very little capability to answer privacy queries within the voice interface [4, 23]: in many cases they don't understand or offer coherent responses to these queries at all, and when they do understand, they often shunt users to mobile apps or websites to read privacy information. Researchers have suggested that adding conversational privacy functionality could potentially mitigate user mistrust about the data practices of CUIs [5].

Researchers have begun to build early-stage prototypes of conversational agents that could handle privacy queries. In 2016, Harkous et al. proposed PriBot, a conversational agent that could engage with users to help them understand privacy policies and other disclosures [15]. In 2022, Bruggemeier et al. published (possibly the first) user study evidence of the effectiveness of conversational privacy prompts. They found that such prompts may positively impact users' perceptions of a system's security and privacy (compared to a CUI that does not prompt users about available privacy choices), and that users may be interested in making privacy choices using conversational mechanisms [5]. However, as of January 2022, no studies (to my knowledge) have compared conversational privacy approaches to more traditional notice and choice paradigms.

2.4 Privacy concerns surrounding voice assistants and smart speakers

Pew Research Center found in the 2019 American Trends Panel that 54% of smart speaker owners were somewhat or very concerned about the data that their devices collected, that less than half actually wanted their smart speakers to behave in more personalized ways, and that even fewer were interested in that personalization *if that meant the smart speaker would collect more personal information* [2, 6].

While a substantial proportion of users of these devices seem to be concerned about data collection, the available data indicates that users rarely use the privacy controls that are available on these devices [1, 18], which I would hypothesize is driven to a significant extent by usability or discoverability challenges.

2.5 Voice interface design: research methodology and design best practices

-
-

Chapter 3

Previous work

3.1 Past privacy choice research

Prior to the independent research that I describe later in this document, I worked on multiple collaborative projects related to privacy choices that have informed and shaped my ongoing and future work [7, 12, 13, 14]:

Identifying user needs for advertising controls on Facebook. Hana Habib, Sarah Pearman, Ellie Young, Ishika Saxena, Robert Zhang, and Lorrie Faith Cranor. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6, Issue CSCW1. 2022. In this study, we conducted an exploratory survey to gather descriptive statistics about users' self-reported concerns and actions related to ad controls on Facebook, and then we conducted a remote, moderated user study to gather observations regarding the usability of these controls. We found that users did wish to control aspects of advertising on Facebook, some of which can currently be controlled using Facebook's current controls; however, users were not always aware that there was a way to act on these wishes, highlighting discoverability problems. Based on our qualitative analysis, we also described four groups or types of users based on privacy concerns, objectives, and willingness to engage with ad controls, and we ultimately provided recommendations for improving the ad controls on Facebook and similar platforms.

"It's a scavenger hunt": Usability of websites' opt-out and data deletion choices. Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Conference canceled due to COVID-19. 2020. Video presentation recorded by Sarah Pearman. We conducted a lab study with 24 participants to observe users interacting with privacy chioces on various websites. We found that users struggled with these interactions, especially actions that required visiting a privacy policy page to find opt-out information. Users struggled to take actions on their own and often looked for assistance on help pages or contacting customer service by email. Overall, we concluded that opting out of data collection or marketing via interfaces such as privacy settings pages and privacy policy pages is difficult for users, and we provided recommendations for improving these choice

interfaces.

Informing the design of a personalized privacy assistant for the internet of things. Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 2020. We conducted 17 semi-structured interviews to explore users' perceptions of Personalized Privacy Assistants (PPAs). Participants' preferences varied, and in considering how much they would want PPAs to automate privacy decisions, participants grappled with the desire for control versus the risk of cognitive overload. The primary recommendation that we made based on these findings was to give users flexibility and choices about the level of automation that a PPA would provide.

Away from prying eyes: Analyzing usage and understanding of private browsing. Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security* (SOUPS 2018). August 12-14, 2018. Baltimore, MD, USA. In this study, we analyzed *in situ* browsing data from over 450 participants in the Security Behavior Observatory (SBO) to better understand users' private browsing behaviors, and then we combined that observational data with a follow-up survey that was administered to both SBO participants and a sample from Mechanical Turk to understand how self-reported private browsing behaviors compared to actual behaviors. We observed participants using private browsing for a variety of reasons, from viewing adult content to making sensitive searches to streaming audio and video. One of the main takeaways from this study that is relevant to my ongoing and future research was that participants overestimated how much private browsing could protect them from online tracking or targeted advertising, supporting concerns about participants' ability to understand the online behavioral advertising ecosystem and protect themselves in the ways that they may wish to.

3.2 User-friendly yet rarely read: A case study on the redesign of an online HIPAA authorization

In this study, we described the iterative refinement and evaluation of a consent flow for a chatbot being developed by a large U.S. health insurance company [25]. This chatbot used Google Cloud technology for data storage and natural language processing, and as a result, the company required users to agree to a HIPAA authorization before they could use the chatbot. This was a particularly interesting context to study consent because of the ways in which the chatbot's data practices violated users' expectations (and misunderstandings) of how health data is legally protected in the U.S. In a three-phase interview and survey study, we tested four versions of the consent flow for this chatbot in order to explore whether changes rooted in our empirical observations and recommended best practices could meaningfully improve usability, user understanding, or user sentiment towards the chatbot.

We first conducted three sets of six remote interview sessions in which we observed each set of users interacting with a different prototype consent flow. Prototype 1 was the original version created by HealthCo, Prototype 2 was a version that we simplified and modified to more clearly state data use details, and Prototype 3 was an even further simplified version. Qualitative results from the interviews suggested that Prototypes 2 and 3 could improve on Prototype 1 in usability and understanding.

In the second phase, we analyzed data from 761 participants who had been randomly assigned to use one of the three prototypes tested in the interview study. We asked questions about their experience, their understandings of what they had read, and whether they would be inclined to use such a chatbot if they encountered that consent information in real life. We then displayed the consent information again, asked participants to review it carefully, and asked them again about their understandings of and attitudes toward the chatbot. We found usability benefits to Prototype 3, and users could understand our redesigned prototypes better when asked to review documents carefully, but user understanding was poor across all prototypes on the first pass through the documents.

In the third phase, we surveyed an additional 456 participants to compare users' understandings and opinions of two consent flow prototypes, one of which omitted the word "HIPAA." We also asked questions to further explore what non-experts understood about HIPAA and Protected Health Information (PHI), finding that most respondents grossly overestimated the protections that HIPAA could provide.

Multiple insights from this study may apply more broadly to creating consent flow interfaces and consent documents for tools that handle health data. First, while our refinements did not necessarily improve understanding in the context of a non-privacy-related task, they did seem to improve both overall usability and users' ability to understand the consent documentation if they were prompted to revisit it and read more carefully. While notice and choice best practices and usability studies will not necessarily solve all of the problems inherent to a consent task of this type, we still recommend making changes such as simplifying language, reducing complexity, and drawing special attention to potentially-surprising elements whenever possible.

Second, while the refinements discussed above seem to improve the overall user experience and the *potential* for users to understand consent documentation *if* they read it, we still find that users are unlikely to read and understand these disclosures when they are skimming a document while focused on some other primary task. Importantly, we also find that some of the disclosures we studied are likely to change users' decisions once they understand them. We argue it is important to find ways to highlight main takeaways to users who are unlikely to read every word, and since our refinements were not sufficiently effective in doing this, we argue that researchers and designers should explore more creative approaches to attracting users' attention to disclosures that may violate their privacy expectations.

A third major insight relates to users' inflated sense of confidence in the privacy and security of healthcare data and their lack of understanding of HIPAA, both of which suggest a need for extreme care in data use disclosures in healthcare contexts.

Our findings help to inform the design of healthcare-related data sharing notices specifically, as well as provide insights on improving the effectiveness of privacy notices in a broader set of contexts.

Chapter 4

Ongoing and future work

4.1 Ongoing work: A conversational approach to mobile app signup and onboarding

4.1.1 Overview

In this study, I will test a more conversational and interactive approach to providing privacy information to users in the context of signup and onboarding for a social media app. The approach I am testing is inspired by non-traditional privacy interfaces encountered in the wild, such as interactions seen in gaming contexts.

4.1.2 Research questions and hypotheses

I will be comparing the following five versions of a prototype across multiple metrics. All versions of the interface will ultimately make the same pieces of privacy information available, but the interactions necessary to acquire that information will vary.

- "Minimal/Conversational": A prototype with a minimal blurb of privacy information on each screen, with a link to a conversational privacy interface for more information
- "Minimal/Policy": A prototype with a minimal blurb of privacy information on each screen, with a link to Terms of Use and Data Policy at the bottom of each screen
- "Zero/Conversational": A prototype with no privacy information on the screen where the data is requested, with a link to a conversational privacy interface for more information
- "Zero/Policy": A prototype with no privacy information on the screen where the data is requested, with a link to Terms of Use and Data Policy at the bottom of each screen
- "Maximal": A prototype that just offers *all* of the available privacy information about a data point in small text on the screen where it is requested, rather than offering additional links to obtain more privacy information

I will gather qualitative and quantitative data focused on the following items from the framework proposed in Hana Habib's thesis [11]: user needs, user ability and effort, user awareness, user comprehension, and user sentiment.

My primary hypotheses are focused around the idea that the conversational approaches, particularly the minimal/conversational approach, will yield better user sentiment and understanding when compared to the policy-based approaches. Conversational approaches are also expected to better meet user needs and allow users to find information with lower effort. It is not clear how user awareness will be affected by this less traditional type of interface, so analysis of this point will be primarily exploratory and qualitative. I expect that effects on awareness will be highly dependent on how the conversational privacy interface is introduced (e.g., if the user reaches that user interface using a link, how is that link worded, and do certain wordings help users to understand what that link might lead to?).

4.1.3 Methods

App prototypes

I have constructed five versions of a prototype of a social media signup interface. This interface presents an imaginary social media app called "Frindle" that requests the following information on signup, with each of the following bullet points being requested on a distinct screen:

- First and last name
- Birthday
- Gender/pronouns
- Phone number *or* email
- Password
- Camera and microphone permissions (in the context of recording a video)

Like Facebook, Frindle requires users to give their first and last name and real-life identity. In terms of content, it is presented as being an app more in the style of TikTok, where sharing short videos is a primary focus.

I built these medium-fidelity prototypes in Adobe XD. They are clickable but not fully functional: for example, they do not allow users to actually type information into form fields.

Phase 1: Qualitative

In the spring of 2022, I have been running remote, moderated user study sessions in which users perform tasks using the prototypes. I then ask users semi-structured interview questions about the experience of interacting with the prototype.

Thus far, participants have been recruited using "Gigs" posts on Craigslist in the Pittsburgh, PA; Cleveland, OH; and Knoxville, TN regions. Potential participants fill out a screening survey including demographic questions and basic technology usage questions (e.g., type of smartphone used). I am using purposive sampling to maximize the demographic diversity of the participants that are invited to participate. Potential participants selected from the screening data are then invited to fill out a consent form, after which they are directed to a Calendly link to sign up for an interview timeslot.

Users are randomly assigned to one of five conditions to determine which prototype they see. To try to distribute participants with technical expertise evenly across the conditions, I performed

a separate randomization process for the participants who reported having any formal education or work experience in a technical field.

These interviews last from about 45 minutes to an hour. Participants are asked to imagine that they are signing up for a new social media app in real life and to interact with the prototype to proceed through the signup process. I do not say anything to prime participants to think about privacy when this scenario is introduced. We do this in a "think aloud" style where, for each screen, participants are asked to explain the options that they see, describe what they think would happen if they selected those options, and then explain what option they would choose next.

I then ask followup questions related to topics including their sentiments about the overall experience, their understanding of how the different data types that the app asked for might be used and shared, their usual behavior surrounding privacy information and privacy policies, and their needs and preferences.

4.1.4 Progress update and preliminary results

As of the time of my proposal presentation, I have interviewed 16 participants. This includes four participants who saw the "Maximal" prototype version, and three each for the other versions of the prototype.

4.1.5 Future plans

Interview data. Since I only conducted a quick, relatively surface level analysis of the interview data that I collected in spring 2022, I will likely make another inductive coding pass through the existing interview data to observe any themes related to privacy needs or sentiments that I did not acknowledge in my first pass through this data.

I may also run additional interviews to acquire a relatively diverse group of four or five participants per condition, with the goal of at least having enough participants to identify any usability issues in each prototype that could distract from the privacy issues that are the focus of this study [22], as well as to elicit additional privacy needs and concerns that may be relevant to ask about in the followup survey.

Followup survey. Before my hiatus from academia that will begin in June, I plan to finish drafting this survey. I have a rough draft at this time, and intend to finalize that and get IRB approval for the final version before the end of May 2022. The primary goal of this survey will be to elicit quantitative comparisons between the prototypes on outcomes related to user needs, ability and effort, awareness, comprehension, and sentiment. We will also collect data about participants' actual behavior in interacting with the prototypes and conduct comparisons across conditions on behavioral outcome variables including whether participants did or did not choose to visit supplementary privacy information screens.

In this survey, participants will first be asked to sign up for the Frindle social media app (a non-privacy task, to avoid priming them to pay extra attention to privacy information). We will collect log data as they do that, and then we will ask followup questions in a Qualtrics survey after the task has been completed.

I will recruit for this survey on Prolific, with gender and age balancing mechanisms in place to ensure the sample is not overly skewed in spite of recent disruptions to the Prolific participant pool [19]. I will perform power analysis to determine the exact sample size once the survey is fully complete and we know what statistical comparisons will be necessary. I will conduct informal pilots to determine the amount of payment that participants will receive based on the amount of time the survey is expected to take. I expect it to be approximately a 10-15 minute survey, and I will aim to pay participants an amount proportional to $15/hour.

In summer 2022, the CUPS lab will have an assortment of student research assistants, and I am hoping that we can assign one of these research assistants to build a medium-fidelity, clickable web version of each prototype that can be deployed on the CUPS server. This will allow us to collect log data about what privacy information screens participants choose to visit when completing the initial task, as well as the amount of time spent on each privacy information screen.

Once the web prototypes described above have been deployed, which should be possible by fall 2022, the survey can be launched to collect the necessary data by the end of 2022. I may perform some of the quantitative and qualitative analysis for this survey data while I am on leave, and I will complete that analysis when I return to finish my dissertation.

4.2 Future work: Enabling voice assistants to have robust privacy conversations

4.2.1 Overview

Past work, including some of my own described in the previous chapter, has shown that the existing notice and choice paradigm often fails to meet user needs and that incremental changes within that paradigm will not always substantially improve user comprehension or attitudes towards their decisions. We also know that current standard approaches to privacy cannot be implemented on many Internet of Things devices, wearables, voice interfaces, or other emerging technologies without a disruptive switch in modalities. Users are thought to be unlikely to read privacy information that is "decoupled" from the main interface [8, 27]. If our existing GUI-focused notice and choice paradigm is already failing users in traditional GUI contexts, we can reasonably predict that trying to apply traditional notice and choice approaches to emerging technologies will not serve users' needs well, and based on the data we currently have about voice assistants and smart speakers, this prediction seems to be holding true.

In this study, I am interested in prototyping and testing a conversational privacy interface that does not switch modalities and instead integrates smoothly with the rest of the capabilities of a voice assistant to give users easy access to privacy information and privacy choices. I intend to collect qualitative data to assist in the design process and then to gather quantitative data to compare this approach to existing voice assistant interfaces that use predominantly decoupled approaches to answering privacy queries (if they can answer them at all).

Question asked	Amazon Echo (Alexa)	Google Home (Assistant)
"Can people [employees] listen to my recordings?"	*Not understood*	*Not understood*
"Who can listen to recordings?"	*Not understood*	*Not understood*
"Change my privacy settings"	Directed to mobile app	Directed to URL
"Tell me about your privacy settings"	*Not understood*	Directed to URL
"Read me your privacy policy"	Directed to mobile app	Directed to URL

Table 4.1: This table demonstrates that, at the time of data collection in the spring of 2020, Alexa and Google Assistant did not allow users to access these privacy details or settings through the voice interface—in fact, they often failed to understand privacy questions at all.

4.2.2 Background: Known problems with VUI privacy interfaces, and proposed solutions

In the spring of 2020, I completed a course project related to the availability of privacy information from voice assistants and smart speakers as part of the Telling Stories with Data mini course at Heinz [23]. The presentation and artifacts for this project are publicly available.

As mentioned in Chapter 2.4, users of smart speakers often have concerns about the privacy of the data collected by these devices, but they simultaneously seem to rarely take privacy-protecting actions when using these devices, suggesting usability challenges.

As part of my course project, in an approach similar to a cognitive walkthrough, I explored the usability of obtaining privacy information from these devices by speaking a set of privacy questions to an Amazon Echo (Alexa) device and a Google Home device to explore what those questions triggered. The results of those questions are shown in Table 4.1.

Alexa could recognize questions about privacy settings or privacy policies, but it just directed me to the "settings in the Alexa app" for anything beyond a cursory response along the lines of "Amazon takes privacy seriously." It did not offer specific guidance about exactly what settings to look for. It did not understand questions about more specific privacy practices, such as whether Amazon allowed employees to listen to recordings.

Google Assistant was similar in terms of the set of questions it could or could not understand. It understood a question about privacy settings that Alexa did not understand, but this wasn't an exhaustive test, so that result might have been reversed if I had a different voice or phrased it slightly differently. Instead of directing me to the Google Home app, the Google device would often direct me to a URL. This alone would not be a very usable solution, but Google Assistant also automatically texts the URL to the associated smartphone when it does this, which was helpful.

This is of course not an exhaustive test, and to study this more closely, I would need to refine this approach, including testing different phrasings of questions and using different speaker voices. However, it's clear in any case that it's not easy to get privacy details from these two voice assistants, and I (a relatively expert user) couldn't find a way to change the privacy settings through the voice interface. The only exception noted at the time of that data collection was that Alexa would allow the user to request the deletion of the last utterance that the user spoke.

More information about my methods and findings is available in a Shorthand report [23], and

additional details and artifacts can be found on Github [24].

Some users may prefer to interact with settings in a visual interface anyway, but generally speaking, our current understanding of notice and choice indicates that a decoupled approach like this tends to be less desirable and more challenging for users. To improve usability—and also to maximize the accessibility benefits of voice assistants—it would make sense to offer the option of getting some privacy information through the voice interface wherever possible, and to enable the voice assistant to understand and give intelligible responses to at least basic questions about privacy practices and settings.

In the fall of 2021, in Dr. Patrick Carrington's Accessibility course in HCII, I worked with Luke Zhang to build a low-fidelity prototype of an Alexa Skill to demonstrate how smart speakers might be able to handle these questions while remaining in the voice modality. A demonstration of this prototype is available via Google Drive.

4.2.3 Background: Testing prototypes of voice interfaces for consent tasks

In the fall of 2020, I also assisted in supervising a team of Privacy Engineering master's students who, for their capstone project, created a prototype of an Alexa Skill privacy interface. Similar to the chatbot consent flows described in Chapter 3.2, this prototype was designed to handle HIPAA-related consent tasks for customers of a large health insurance company. The prototype's voice interface consent flow would begin with a question such as, "Can Highmark disclose your Protected Health Information, AKA 'PHI'¿' It was then able to offer explanations of relevant concepts if users asked for more details [10].

This Alexa Skill prototype was tested in 12 interview-style remote user study sessions. Overall, the researchers reported that participants often felt positively about the voice interface from a privacy perspective and that most would be willing to use such a product if it existed in real life. A few participants specifically noted that they had never read privacy policies before but that the condensed policy information offered by the voice interface was digestible and useful to them. Participants also thought the ability to revoke data sharing permissions through a voice interface gave them more control over their data [10].

The researchers also noted downsides to this voice-based approach to consent. Some users who didn't care about privacy found it annoying to have to respond to the voice interface's questions instead of just proceeding to the primary task, and one user said that using a mobile application to complete this interaction would be acceptable, with no need for this to be a voice-based process. Furthermore, when users asked for more details, they sometimes complained that the length of the response from the voice assistant was too long, Some also found the way that the voice assistant responded to be repetitive. From a privacy perspective, one interesting concern that arose was that the voice assistant might not be able to verify the identity of the user, meaning that unauthorized people with physical access to the smart speaker might be able to make unwanted changes to privacy settings. Additional usability and privacy are described in the capstone team's report [10].

Feature	Data types involved
Reminders of habits such as meditation or yoga	Calendar permissions, mood detection via voice
Reminders of doctors' appointments, fitness training, and other health-related events	Calendar permissions
AI-guided talk therapy [26, 28]	Mood detection via voice [16], collection of "trigger words" to study users in aggregate [20]
Hands-free workout guidance	Permissions to sync with fitness wearables to obtain data such as heart rate
Hands-free recipe instructions	[Minimal extra data needed]

Table 4.2: This table lists health features that the Alexa Skill used in this study might offer, as well as data types that might be necessary for such a feature to function. This list of possible features will be employed in developing study protocols, prototypes of voice interactions, and consent flows. All of these features might also require other permissions such as the ability to sync with the Alexa app and health apps on the user's mobile phone, the ability to distinguish one user's voice from voices of other users/household members, and so forth.

4.2.4 Proposed methods [tentative / subject to change]

I will focus on Amazon Echo devices with the Alexa voice assistant for this study, and I will explore how conversational flows native to the voice interface modality may compare to decoupled approaches to answering privacy questions and obtaining consent. I intend to explore a scenario in which users might encounter requests for their data where it would be appropriate for the voice assistant to ask for consent, and in which users might also initiate questions or settings changes of their own. The ideal scenario to explore would also be one with some amount of ambiguity or tradeoff, i.e., one that we would expect some users to be comfortable with and other users to be uncomfortable with, and some to be comfortable with only under certain conditions. This is likely to be more informative than a very innocuous situation where most users who would use a voice assistant would grant data access, or a situation where the voice assistant requests a type of data collection or use that most people would find overly invasive.

Given that some of my past work has looked at consents in health-related apps, and that health-related technologies (a broad umbrella including apps focused on "fitness" and "wellness") are both useful and prone to collecting a lot of potentially sensitive data, I will use an imaginary health app or Skill as the example scenario here. This app could offer features such as those shown in Figure 4.2 which might, respectively, require the listed data types. Figure 4.2 also includes citations indicating examples of Alexa Skills that currently offer similar features or research indicating that these types of voice features are being developed.

Before designing an interface, I would obtain data about how people talk about these topics naturally, so that the voice flow could be designed to mirror how humans naturally converse about

privacy as much as possible. I would likely first run a set of qualitative study sessions in which I gave people a task that caused them to ask questions about privacy information. One option for how this could be done would be to give them a functioning smart speaker or other voice assistant, with its base software, and ask them to do a privacy task with it. However, since (as of 2022) most of these assistants can't handle many privacy interactions in the voice interface, this might have limitations. In this case, I would need to come up with some other task to elicit more examples of how people would do this *if* the interface functioned fully.

Next, I would have people try to interact with a functioning prototype of an Alexa Skill informed by the findings from the previous phase, and I would gather qualitative data about the usability and users' perceptions.

Finally, I would run a larger study (most likely online via Qualtrics or an unmoderated user study platform) to get quantitative comparisons of this interface versus existing decoupled approaches. I would use questions and metrics related to users' needs, ability and effort, awareness, comprehension, and sentiments.

Chapter 5

Thesis outline

5.1 Introduction

5.2 Background and related work

5.3 Past privacy choice research

5.4 User-friendly yet rarely read: A case study on the redesign of an online HIPAA authorization

5.5 A conversational approach to mobile app signup and onboarding

5.6 Enabling voice assistants to have robust privacy conversations

5.7 Conclusion

Chapter 6

Dissertation timeline

6.1 Leave/ABS time

Beginning June 2022, I will be working a full-time UX research job and will go on leave or register for ABS status. I will continue checking in with Lorrie biweekly (potentially async) and will work on the following items:

- ☐ June 2022 – December 2022: Read and summarize one paper per week for Related Work
- ☐ January 2023 – July 2023:
  - ☐ Ideate and plan for third study
  - ☐ Start preparing IRB protocol for Study 3

6.2 Return to CMU full-time or part-time, possibly August 2023

I will work that job for at least a year but after 1-2 years plan to return. I may return full-time if CMU's remote work policies evolve to allow for this, since I expect to be living in Tennessee at that point. I will also consider finding a part-time industry job that would allow me to work on my dissertation part-time while remaining in ABS status.

The timeline below is really tentative and subject to change. Overall, the goal would be to finish in a year (two semesters and a summer) or maybe just two semesters, if I'm back full-time. If I finish while working part-time, this timeline will be structured differently.

- ☐ August 2023: Finalize and submit IRB protocol for Study 3
- ☐ September 2023: Begin data collection for Study 3
- ☐ October – November 2023: Data analysis
- ☐ December 2023: Write up Study 3 findings in thesis document
- ☐ January – February 2024: Iterate on other sections of thesis document
- ☐ March 2024: Final iterations with Lorrie/committee

☐ Before end of spring semester 2024: Defend (and find a job)

Bibliography

[1] Tawfiq Ammari, Jofish Kaye, Janice Y. Tsai, and Frank Bentley. 2019. Music, Search, and IoT: How People (Really) Use Voice Assistants. *ACM Transactions on Computer-Human Interaction* 26, 3 (June 2019), 1–28. DOI:http://dx.doi.org/10.1145/3311956 2.4

[2] Brooke Auxier. 2019. 5 Things to Know about Americans and Their Smart Speakers. (Nov. 2019). https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/ 2.4

[3] Omri Ben-Shahar and Adam Chilton. 2016. Simplification of Privacy Disclosures: An Experimental Test. *Journal of Legal Studies* 45 (June 2016), 27. https://www.ftc.gov/system/files/documents/public_comments/2017/11/00022-141740.pdf. 1, 2.1

[4] Birgit Brüggemeier. 2020. Communicating Privacy and Security in Conversational User Interfaces. (Dec. 2020). https://mediaserver.eurecom.fr/permalink/v125f76418ddcf52uewo/iframe/ 2.3

[5] Birgit Brüggemeier and Philip Lalone. 2022. Perceptions and Reactions to Conversational Privacy Initiated by a Conversational User Interface. *Computer Speech & Language* 71 (Jan. 2022), 101269. DOI:http://dx.doi.org/10.1016/j.csl.2021.101269 2.3

[6] Pew Research Center. 2019. *2019 Pew Research Center's American Trends Panel: Wave 49, June 2019, Draft Topline*. Technical Report. Pew Research Center. https://www.pewresearch.org/wp-content/uploads/2019/11/FT_19.11.21_SmartSpeaker_methods-topline-final-11.21.pdf 2.4

[7] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:http://dx.doi.org/10.1145/3313831.3376389 3.1

[8] Federal Trade Commission. 2015. *Internet of Things: Privacy & Security in a Connected World*. FTC Staff Report. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-

privacy/150127iotrpt.pdf 4.2.1

[9] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO, USA, 21. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck. 1, 2.1

[10] Chenxiao Guan, Chenghao Ye, Yigeng Wang, and Fangxian Mi. 2020. *Exploring Consent and Authorization Voice Interface for Healthcare Privacy*. Carnegie Mellon Privacy Engineering Master's Program capstone report. https://github.com/oddguan/highmark-alexa/blob/4ee1e89e7c9676e2bcbba62c7eb5e64fbe14cec3/final%20report.pdf 4.2.3

[11] Hana Habib. 2021. *Evaluating the Usability of Privacy Choice Mechanisms*. Doctoral Thesis. Carnegie Mellon University. https://www.hanahabib.com/assets/docs/Thesis_Document.pdf (document), 1, 4.1.2

[12] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD, USA, 18. https://www.usenix.org/system/files/conference/soups2018/soups2018-habib-prying.pdf 3.1

[13] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. DOI:http://dx.doi.org/10.1145/3313831.3376511 3.1

[14] Hana Habib, Sarah Pearman, Ellie Young, Ishika Saxena, Robert Zhang, and Lorrie Faith Cranor. 2022. Identifying User Needs for Advertising Controls on Facebook. In *Proceedings of the ACM on Human-Computer Interaction (CSCW1)*, Vol. 6. 3.1

[15] Hamza Harkous and Kassem Fawaz. 2016. PriBots: Conversational Privacy with Chatbots. In *Workshop on the Future of Privacy Indicators, at the Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016*. 2.3

[16] Khari Johnson. 2019. Amazon's Alexa May Soon Know If You're Happy or Sad. (July 2019). https://venturebeat.com/2019/07/08/amazons-alexa-may-soon-know-if-youre-happy-or-sad/ 4.2.4

[17] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 2009)*. Association for Computing Machinery, New York, NY, USA, 1–12. DOI:http://dx.doi.org/10.1145/1572532.1572538 1, 2.1

[18] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listen-

ing?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–31. DOI:http://dx.doi.org/10.1145/3274371 2.4

[19] Rafi Letzter. 2021. A Teenager on TikTok Disrupted Thousands of Scientific Studies with a Single Video. *The Verge* (Sept. 2021). https://www.theverge.com/2021/9/24/22688278/tiktok-science-study-survey-prolific 4.1.5

[20] Helen Lock. 2018. This AI Therapy Skill for Alexa and Google Aims to Help with Everyday Mental Health. (Oct. 2018). https://www.the-ambient.com/features/mindscape-alexa-therapy-skill-mental-health-1034 4.2.4

[21] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* (2008), 22. http://www.is-journal.org. 1, 2.1

[22] Jakob Nielsen. 2012. How Many Test Users in a Usability Study? (June 2012). https://www.nngroup.com/articles/how-many-test-users/ 4.1.5

[23] Sarah Pearman. 2020a. Smart Speakers & Privacy Choices. (2020). https://carnegiemellon.shorthandstories.com/smartSpeakerPrivacy/ 2.3, 4.2.2, 4.2.2

[24] Sarah Pearman. 2020b. Smart Speakers & Privacy Choices. (2020). https://sarahpearman.github.io/data-stories/final-project-main.html 4.2.2

[25] Sarah Pearman, Ellie Young, and Lorrie Cranor. 2022. User-Friendly yet Rarely Read: A Case Study on the Redesign of an Online HIPAA Authorization. In *Proceedings on Privacy Enhancing Technologies (PoPETS)*. 3.2

[26] PromethistAI a.s. Poppy's Place. PromethistAI a.s.. (????). https://www.amazon.com/PromethistAI-a-s-Poppys-Place/dp/B08YJK1QVT 4.2.4

[27] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)*. USENIX Association, USA, 1–17. 4.2.1

[28] The OT Toolbox. 2017. Alexa Skills for Therapy. (April 2017). https://www.theottoolbox.com/alexa-skills-for-therapy/ 4.2.4