Empowering Resignation

There's an App for That

John S. Seberger
Indiana University Bloomington
Bloomington, Indiana
jseberge@indiana.edu

Marissel Llavore
Indiana University Bloomington
Bloomington, Indiana
mllavore@iu.edu

Nicholas Nye Wyant
Indiana University Bloomington
Bloomington, Indiana
nnwyant@indiana.edu

Irina Shklovski
University of Copenhagen
Copenhagen, Denmark
ias@di.ku.dk

Sameer Patil
Indiana University Bloomington
Bloomington, Indiana
patil@indiana.edu

ABSTRACT

"There's an app for that" is perhaps *the* definitive rhetoric of our times. To understand how users navigate the trade-offs involved in using apps that support a variety of everyday activities, we conducted scenario-based semi-structured interviews ($n = 25$). Despite the technical and regulatory mechanisms that are supposedly meant to empower users to manage their privacy, we found that users express an overarching feeling of resignation regarding privacy matters. Because these apps provide convenience and other benefits, as one participant put it, "there is a very fine line" that marks the divide between feeling empowered in the use of technology and coping with the discomfort and creepiness arising from invasive app behavior. Participants consistently expressed being resigned to disclose data even as they accepted personal responsibility for their own privacy. We apply the findings to discuss the limits of empowerment as a design logic for privacy-oriented solutions.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; *Empirical studies in collaborative and social computing*; *Empirical studies in ubiquitous and mobile computing*; • **Security and privacy** → **Social aspects of security and privacy**.

KEYWORDS

privacy, privacy controls, privacy management, privacy preferences, creepiness, discomfort, resignation, power, empowerment, smartphone apps, mobile apps, usage scenarios, conditional empowerment, hyperbolic scaling

ACM Reference Format:
John S. Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering Resignation: There's an App for That. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445293

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05.
https://doi.org/10.1145/3411764.3445293

1 INTRODUCTION

"There's an app for that" is perhaps *the* definitive rhetoric of our times. Whether keeping in touch with your friends, monitoring your coffee pot, or keeping track of your running route, apps form an infrastructure that can empower as well as exploit [61]. The sheer proliferation of apps has caused many a headache in the privacy and security research community given the built-in, often predatory, data extraction capacities driven by advertising revenue. Researchers have worked on a variety of approaches to warn users about the privacy dangers of various apps and to encourage users to exercise selectivity in app use. Some have attempted to simplify End User License Agreements (EULAs) or nudge users toward safer behaviors, while others have focused on developing privacy enhancing technologies (PETs) intended to intervene in unwelcome data disclosures. While there is ongoing debate about the success of these efforts [24, 91, 97], researchers continue to demonstrate that people tend to ignore EULAs [32] and even those who download PETs tend to be inconsistent in their use of them [43].

Apps might promise a better and more convenient life by enabling people to do useful things, but they demand personal data in return. The question remains whether it is possible to enjoy the benefits of such apps while limiting the invasiveness and other undesired aspects of their operation. The privacy community's Herculean efforts to address the burgeoning privacy issues of the app ecology typically hinges on the idea of empowering users to take responsibility for managing their own privacy. However, these efforts often fail due to great levels of resignation about the state of the predatory data economy. Empowerment, after all, is not necessarily a liberating experience when it results in shifting responsibility onto individuals by ostensibly giving them tools to take control without changing the structural conditions of the situation [50]. The discrepancy between people's expressed privacy concerns and their real-world actions related to their data (i.e., the privacy paradox) remains a persistent issue. This attitude-behavior gap continues to confound technologists, politicians, and researchers alike [72, 109]. Whether we should believe what people say or point to the privacy paradox and follow what they do is not a straightforward decision. The rapid development of the contemporary data economy is driven by following the latter route [25, 117], based on the underlying assumption that data about privacy-related behavior speaks for itself, even if the behavior does not match what people *say* they might want.

So why can't Johnny do the "right" thing and manage digital privacy? Some researchers have argued that people feel helpless and resigned in the face of data demands and accept the discomfort caused by inevitable privacy violations [25, 91]. Others have pointed out that privacy in Human Computer Interaction (HCI) is mismeasured or misdefined, thus leading to solutions that fail to address the core problem [12, 21]. Despite decades of research and debate across many different fields, a clear and coherent definition of privacy continues to be elusive [21, 101]. Privacy not only means different things in different contexts [66, 94], but has both affective [99] and cognitive dimensions. The conceptual heterogeneity of privacy complicates the appeals to rationality that dominate some research threads in usable privacy. As digital technologies become ever more personal, invasive, and creepy, it is imperative that we pay attention to the affective dimension of privacy violations.

We explored the affective experiences and discomforts associated with data-oriented apps by asking participants to engage with and react to a set of semi-fictional scenarios of everyday app use. These scenarios were deliberately calibrated to elicit discussion of real-life experiences, yet violate expectations and vary feelings of control over data disclosure. We engaged in this research to answer the following research questions:

- **RQ1:** How do people manage responsibilities for data disclosure as a result of app use?
- **RQ2:** How does feeling empowered to control different aspects of data disclosure mitigate feelings of discomfort in the face of privacy violations?

Our findings demonstrate a paradoxical relationship between empowerment and resignation that arises from the provision of end-user privacy controls and the perceived pervasiveness and inevitability of privacy violations. Drawing on prior work about digital resignation [25], we develop the concept of *conditional empowerment*. Conditional empowerment refers to a limited achievement of control tempered by justifications for the inability or unwillingness to exercise such control to its full extent. We additionally identify and define the phenomenon of *hyperbolic scaling*, which contributes to people's sense of privacy fatalism and resignation in the context of conditional empowerment. As a result, the current forms of privacy-related empowerment ironically encourage further resignation and acceptance of unabated data disclosure. In the context of end-user privacy control, attempts to empower end-users are ultimately disempowering.

Based on these findings, we make the following contributions:

- clarifying the importance of paying attention to affect when studying privacy-related experiences of technology use;
- demonstrating the application of the concept of empowerment to the privacy discourse by disambiguating how different forms of power complicate technology use; and
- developing novel concepts of conditional empowerment and hyperbolic scaling to reconceptualize traditional discussions of the privacy paradox and individual responsibility for data management.

In the sections that follow, we present an overview of the literature on privacy, creepiness, resignation, and empowerment in HCI and beyond. We then describe our method and proceed to an in-depth presentation of the findings. We apply the insight gained from the findings to offer implications of the affective dimension of privacy for research and system design in usable privacy specifically, and in HCI more broadly.

2 RELATED WORK

Nearly a decade ago, King et al. [46] asked: "Privacy, is there an app for that?" Their study was concerned with the proliferation of third-party apps on the Facebook platform and the challenges it presents for end-user privacy management. They found that privacy-related decision making is not affected by the level of understanding about apps and their inherent privacy threats but is dependent on whether a user had an adverse privacy experience with apps. Since the publication of King et al.'s [46] research, apps and the various platforms that power them have essentially colonized everyday digital experience. People's decisions regarding installing particular apps or evaluating their privacy threats has become a burgeoning area of research (e.g., [20, 44, 49, 111]). One of the major thrusts in this area is the development of mechanisms that ostensibly empower people to make privacy-related decisions about app use and data disclosure.

2.1 Affective Components of Privacy

Privacy has been defined variously as the control over personal data [65, 109], a taxonomy of harm to individuals or groups [94, 95], the management of personal boundaries [6, 79], a matter of confidentiality [24, 78], a social issue [57], a relational practice [10, 68], a socially negotiated form of power [69], or appropriate data use in situated contexts [71]. While some definitions focus on individual decision-making and cost-benefit analyses [57, 65, 78, 94, 95, 109], others describe mechanisms that include normative [71, 79], relational [6, 10, 21, 68, 69], and affective facets [69, 99]. As McDonald and Forte [61] note, each definition of privacy is political, thus necessitating a careful examination of the choices underlying its characterization. For example, McDonald and Forte [61] argue that, in being normative, the theory of contextual integrity [70, 71] privileges the rights and expectations of certain users over others and systematically, if unintentionally, excludes vulnerable populations.

The HCI privacy research community has worked on finding ways to help users manage data disclosure in digital contexts in spite of the lack of a common definition of privacy. Research continues to show that people have trouble understanding privacy policies, despite efforts to increase transparency [48] and user awareness of personal data collection [30]. Users rarely adopt recommended security and privacy practices despite nudges [86, 100, 103] designed to encourage such behavior [59]. Even when users engage in privacy- and security-preserving behavior, they frequently abandon these practices in the long run [116]. Ultimately, privacy policies are relatively ineffective in motivating and enabling people to make informed data disclosure decisions even if the information is delivered in a context-specific manner [26].

Delivering privacy notices and communicating related user choices is a common theme in canonical privacy studies (e.g., [4, 22, 73]). Recent work suggests self-management of privacy is overly burdensome [37, 96], even when users are ostensibly empowered through the provision of "soft paternalistic" [2] PETs or nudged toward privacy-preserving behavior [100]. In one estimation, the burden of

self-management arises because users simply cannot meet the cognitive demands of managing non-standardized privacy settings across contexts [3]. The phenomenon of security fatigue adds further complexity [29] by diminishing people's ability to make decisions [98] even where good decisions are possible.

In order to re-approach the value of such concepts as choice [18] within the framework of privacy self-management, it is necessary to understand the broader context within which choice is embedded. Prior work has shown that empowering users to manage their own privacy might paradoxically render them more susceptible to privacy violations [15]. Given the complexity and cascading nature of privacy choices [5], there is a need for a deeper understanding of the affective and social power structures and the sociotechnical context within which such cascades play out [52].

Media coverage of privacy issues [89] and informal stories about other people [83] play an important role in privacy decisions, serving as informal lessons or behavioral heuristics. Further, perceptions of technology are influenced by prior experiences with security technologies and the data-driven inferences made by the platforms [82]. Idiosyncratic understanding of the prevalence of malicious entities, such as hackers and viruses, influence perceptions of privacy and the behavior those perceptions engender [108]. The mental models users develop to understand or rationalize behavioral tracking on major platforms, such as Google and Facebook, directly impact the expression of privacy concerns [81]. These observations underscore the emergence of privacy as a problem that must be addressed, even if the concept of privacy is not precisely understood.

Affect clearly plays a role in behavioral decisions regarding risk [42] and has been theorized as part of a general model of cognitive appraisal relevant to privacy perceptions [54]. Nudging users toward positive affect enhances trust in websites [107]. Emotionally-valenced language may heighten engagement with privacy policies [47]. While the relationship between privacy and affect is generally visible, our understanding of it in a technology-specific context is reduced to "idiosyncratic associations" [41]. The role of affect in privacy deserves more systematic and focused attention in terms of defining the conceptual space and understanding the practices that instantiate the concepts in everyday life.

Privacy is an implicit promise that dignity and respect are parts of end-user relationships constituted by data exchange with platforms and apps. The proliferation of privacy-preserving mechanisms that bestow users control over data disclosure set forth impossible expectations by the underlying platforms [67], leading frequently to the promise of privacy being broken [75]. Everyday technology use is full of privacy trade-offs, and users trade personal data while hoping to avoid adverse outcomes even as they fail to behave in a privacy-preserving manner [40]. When technology use necessarily involves broken promises and dashed hopes, we argue that privacy can be better understood by taking into account the negative affect these practices can generate, including creepiness, frustration, disappointment, and resignation.

2.2 Creepiness and Resignation

In HCI, discomfort with technology use has been considered in various ways [13], but the majority of discussions have focused on privacy concerns because privacy violations are unpleasant experiences. Yet, technology use can cause discomfort just by being creepy, even without explicit privacy violations [76, 91]. Researchers have considered the experience of creepiness as a weak motivation for non-use [115]. Creepiness seems to be connected to the discovery of unexpected flows and uses of personal data in the course of everyday encounters with mundane technology. For instance, participants in many studies of behavioral advertising, location sharing technologies, or data leakage often label discomfiting experiences as creepy [45]. However, studying this inherently-embodied emotional response can be tricky because what is considered creepy often differs across individuals [45].

Because creepiness is an emotional reaction, it is difficult to formulate a concrete definition describing it. In legal scholarship, creepiness is characterized vaguely as individual discomfort with the state of the digital data economy [23]. Tene and Polonetsky [102] note that creepiness is "highly subjective and difficult to generalize," but specify that it may be a response to behavior that "leans in" against traditional social norms. Research in social psychology investigating creepiness in human encounters [53] suggests that feeling "creeped out" is "an emotional response to ambiguity about the presence of threat" [60]. In HCI, creepiness has been defined as "an emotional response to a sense of wrongness that is difficult to clearly articulate" [91]. Recent work exploring the concept of creepiness in technological interactions includes: characterizing the intimacy of whispers when conversing with intelligent personal assistants (IPAs) [77]; developing a taxonomy of technology experiences considered creepy by children [113]; and situating the perceptions of smart home technologies in relation to accepted social norms [80]. As aspects of daily life mediated by technology continues to increase, we observe a corresponding rising trend in the use of creepiness as an analytical concept.

In research on data leakage and privacy, the term "creepy" is frequently used alongside words such as invasive, disturbing, intimidating, unnerving, uncomfortable, and suspicious to indicate a sense of wrongness and discomfort with technologies that tends to put people on edge, even if does not lead them to take drastic action [9, 56, 102, 105, 115]. Shklovski et al. [91] have argued that the lack of response comes from learned helplessness, an internalized feeling of lack of control given the sheer magnitude and variety of data demands. Learned helplessness is a form of resignation directly related to the idea of 'powerlessness' that users feel in relation to the "growing awareness of just how little people know about the ways in which their data might be turned back upon them" [7].

What Draper and Turow term "digital resignation" [25] is learned helplessness that manifests as the internalization of powerlessness in dealing with the conditions created by digital platforms and the surveillance culture associated with them [33]. Digital resignation can be understood as a "21st century malaise" [25] spurned on by surveillance capitalism [117] that emerges in the use of large-scale platforms driven by ad revenue, such as social media and mobile apps. Digital resignation impacts attitudes regarding privacy, leading users to put up with unwanted data disclosures even when they perceive having control over privacy [27]. Resignation can thus act as a counteracting force to efforts to empower users to assert more control over managing their privacy.

2.3 Empowerment: Different Forms of Power

The concept of empowerment in HCI has generally been understood as a technological outcome that allows people to be in control of

their lives in new ways enabled by technology [39]. Despite the prominence of the term, its precise meaning in HCI is as difficult to pin down as that of 'creepiness.' In a recent review of 54 papers that used the concept of empowerment, Schneider et al. [85] structured the use of empowerment as an analytical lens by combining two approaches. The first approach is from community psychology in which empowerment refers to gaining mastery over issues of concern [84]. The second approach is based on the etymological relationship between 'power' and 'empowerment' as an interplay between two central concepts of power: the *power to* act and the *power over* conditions for action [85]. We extend the analysis of Schneider et al. [85] by focusing on these two forms of power.

To define *power to*, Schneider et al. [85] rely on Arendt's [8] notion of power as an individual's capacity to act, which Arendt distinguishes from violence or strength. In the HCI context, however, Schneider et al. [85] see the concept manifesting as technology enabling individuals to accomplish new tasks or achieve existing goals in a better way. In this way, *power to* is more of an augmentation of *capability* that can occur without a greater augmentation in *capacity*. One might achieve the power to do something within a certain context, but that power to do something does not inherently change the context in which it is granted or achieved. For example, users might have the capability to control access to location information, but when apps keep demanding location information frequently, the perpetual need to pay attention to this particular demand can become overwhelming.

In contrast, *power over* builds on the more traditional sociological notion of using power to bend others to one's will. This is a relational concept that speaks to hierarchical interactions among actors where some entities have the power to direct, allow, or limit the actions of others. *Power over* encodes inherent power imbalances and delimits the context within which *power to* can be exercised by individuals. For example, anyone with a Gmail account has the power to receive an email message from anyone who has an email address; however, Google has *power over* the conditions under which that email is received as well as the processing of the content of the email message for advertising and other purposes. *Power to* is often, if not always, nested in various external forms of *power over*. To put it another way, *power to* occurs in relation to an actionable ability while *power over* defines its limits by referring to the context in which that *power to* can be exercised.

The distinction between *power to* and *power over* is essential for understanding people's perceptions of digital privacy and the ostensible empowerment of the end-user via privacy controls. Research in the privacy domain often implicitly explores the give and take between *power to* and *power over*. For example, when Haney and Lutters [35] consider the possibilities of increasing self-efficacy and hope among users confronted with privacy and security issues, they rely on the idea of empowerment. The implicit logic is that users are empowered when they are provided with a privacy policy and given the *power to* specify and regulate their privacy concerns through the manipulation of application settings in accordance with the policy. Such empowerment is about the perception achieved through the creation of positive affect toward security. This perception of the *power to* control one's privacy settings is accurate in so far as users can in fact change the settings. However, that change in capability, whether perceived or real, does not ultimately change user capacity. The actions constituting their *power to* remain bounded by the *power over* exerted by the technology and the actors responsible for its design, development, deployment, and maintenance.

In a similar move, Wu et al. [112] argue that user empowerment regarding privacy should occur through providing users with the *power to* manage privacy according to their own calculus. While Wu et al. [112] point out that "users should be empowered to make personal trade-offs between perceived risk and response cost," they do not consider the nature of the trade-offs from which users might choose. Empowerment through the provision of responsibility ultimately occurs in the context of someone else's *power over*, which defines the limits of individual capacity to act. This observation raises questions about the limits of privacy-oriented solutions that aim to empower individuals by augmenting their agency. Given the complexity and interdependence of networked data infrastructures, it is likely that any attempt to augment the capability of individuals to manage their data will not be successful precisely because this *power to* is always already nested in multiple and overlapping contexts of *power over*.

The *power to* and *power over* dynamic is related to the large-scale digital processes described by Zuboff [117] in her conceptualization of surveillance capitalism. While Zuboff seeks to develop a macro-level argument about changes in capitalism enabled by the rapid development of digital and surveillance technologies, our approach focuses on micro-level distinctions in how individuals deal with privacy concerns when using digital technologies. Attempts to enact the capabilities of control over personal data could lead to frustration and perhaps even resignation as the limits of the capacity to act are discovered. Given the limits of empowerment, we explore the extent to which it can mitigate the discomfort experienced in the face of privacy violations through an empirical investigation to study the relationship between *power to*, *power over*, and digital resignation in practice.

3 METHOD

To investigate affective dimensions of privacy and the role of affective experiences in helping people feel empowered to manage data disclosure, we conducted semi-structured interviews with 25 participants (see Appendix Section B for the interview protocol). Prior research suggests that people often feel guilty and uncomfortable about their privacy practices [91]. Therefore, asking directly about privacy can result in inflated expressions of privacy concern [17]. In order to counter both of these issues, we developed a set of semi-fictional scenarios that made no explicit mention of privacy and asked participants to express their feelings as if they found themselves facing the situation described in the scenario. The construction of scenarios allowed us to manipulate the semantic content communicated to participants such that it included aspects likely to evoke detailed discussion about people's expectations. Participants were free to manage the disclosure of their own practices in their responses. Participants discussed the set of scenarios in the same order during semi-structured interviews. The study procedures were approved by Indiana University's Institutional Review Board (IRB).

3.1 Scenario Construction

Grounding semi-structured interviews in the discussion of scenarios about hypothetical but realistic encounters with technology offers a systematic way of simulating a range of potentially problematic situations. Scenario- and vignette-based methods are frequently used in research on privacy (e.g., [1, 38, 58]). Scenarios have been used to understand phenomena as varied as information-sharing policies in social network sites [28], perceptions and attitudes toward automatic gender recognition [34], and discursive framing of menopause [11], to name just a few.

We developed scenarios through an iterative and collaborative process involving extensive discussion between researchers (see Table 1 for the description of scenarios reported in this paper). We followed Meinert's [63] guidelines for scenario construction to create scenarios that are novel, multifaceted, believable, and never right or wrong. Constructed from contemporary debates about technology in the media, each scenario addressed well-worn privacy concerns, covering a range of common applications that would be familiar to people. The scenarios were intended to confront participants with realistic circumstances that expose potentially unexpected data flows underlying the operation of familiar technologies. Every scenario represents a hypothetical and unexpected data-management issue that can potentially result in unwanted exposure of personal data to various actors. Collectively, the scenarios covered a heterogeneous set of technologies in order to maximize the overall realism of the study. Since people are rarely users of only one application, we engaged them across a range of apps.

Prior work on creepiness has highlighted the importance of three underlying factors: (i) violation of personal boundaries (e.g. [91]); (ii) ambiguity of the threat (e.g. [51, 60]) resulting from boundary violation; and (iii) user control over privacy (e.g. [110, 114]). We constructed scenarios that involve the violation of personal boundaries and manipulated the latter two factors by varying the ambiguity regarding data flows and the level of perceived user control across the scenario set. For example, Scenario 1 (Music ID) sets up user expectations by introducing a familiar type of application: a music-identification app. Although the 'weekly top chart' feature included in the scenario is ostensibly essential to the utility of the app, the mention of the associated targeted advertising hints at the underlying revenue stream. At the same time, the scenario description is intentionally ambiguous about the specifics of data collection, leaving people free to make their own inferences. In this scenario, the user does not have control over the data flows apart from choosing not to install and use the app at all. Overall, Scenario 1 represents a high level of ambiguity and a low level of user control.

3.2 Sample and Data Collection

In the spring of 2019, we conducted a small pilot study ($n = 6$) to test the scenarios and study design, recruiting participants via fliers distributed around the campus of Indiana University Bloomington. The initial sample of six participants involved students and faculty at the university. Analysis of the pilot data demonstrated the efficacy of our scenarios and pointed to potentially interesting insight regarding the relationship between privacy trade-offs and general outlook on app culture. These initial results motivated us to continue the data collection using the same interview protocol.

In the spring and summer of 2020, we recruited 19 participants from a diverse pool of people who completed an initial screening questionnaire (see Appendix Section A). We recruited participants via the web and social media platforms, including Craigslist, Reddit, Facebook, and LinkedIn. The online recruitment facilitated sampling beyond our university community and complying with the physical distancing research protocols necessitated by the COVID-19 pandemic. We used the responses to the screening questionnaire to select a sample diverse in terms of ages, genders, and professions. Across both stages of data collection, we interviewed 25 individuals. Interviews in 2019 were conducted in person and were audio recorded while those in 2020 took place over videoconferencing (i.e., Zoom) and were recorded with audio and video.

Table 2 provides details of the sample. The 25 participants were 21–51 years old, with a median age of 36. Thirteen participants identified as female, ten as male, and two as non-binary. Twelve participants were students, staff, or faculty of Indiana University Bloomington while the remaining 13 covered diverse backgrounds and occupations. Interviews lasted anywhere between 36 to 100 minutes, with an average of 56 minutes. Each person received a $10 Amazon gift card for participating in the study.

3.3 Anonymization and Data Preparation

Prior to analysis, we transcribed the interview recordings using a two-step process. We first obtained a transcript based on automated audio processing by the service Otter.ai. We then verified and corrected the transcription as necessary by manually comparing it with the audio. During the manual verification, we made minor edits, such as removing filler words. This transcription process is broadly in-line with qualitative research best practices [62], resulting in efficiently usable transcripts. We anonymized all transcripts by replacing names with pseudonyms and removing any personally identifiable information. The original recordings were destroyed following the generation of the anonymized transcripts.

3.4 Analysis

We analyzed the interview transcripts using thematic analysis [16] approaches informed by grounded theory techniques [31], with all five authors of the paper involved in the coding process. Our approach was collaborative and iterative, precluding the use of inter-rater reliability since code development was discussed and harmonized by coders throughout the process and by the full team on a weekly basis. Two coders initially coded three transcripts in-vivo using an open coding approach. These coders then compared and discussed the codes with the full research team to harmonize interpretation. Each coder then coded half of the remaining transcripts, periodically harmonizing newly introduced codes and interpretations in collaboration with the full research team. Through extensive code reviews by the full team and the exchange of coder memos throughout the process, we identified initial emergent themes. We further developed and refined these themes through iterative memoing, code co-occurrence analysis and clustering, and weekly team discussions. This process resulted in identifying relationships of interest between the concepts of privacy trade-offs, discomfort, empowerment, and resignation that are described in-depth in the following section.

Table 1: Scenarios used in the semi-structured interviews. *A* and *UC* designate Ambiguity and User Control manipulations, respectively.

Manipulation	**Scenario Text**
1. Music *A*: High *UC*: Low	You have installed an app that can identify music tracks by listening to them. From this, the app creates a 'weekly top chart' of songs you listen to the most. The data about your listening habits is used to tailor music ads within the app. You can't remove the ads.
2. Diet *A*: Low *UC*: Moderate	You have installed an app to help you keep track of what you eat by inputting the food you eat throughout the day. The next day, a friend informs you that the people making the app are selling the collected information to local grocery store chains. You can select which grocery store chains will receive your data.
3. Voice-to-Text *A*: Moderate *UC*: Moderate	You have installed a messenger app that can do voice recordings that you can send instead of text messages. The app has access to your microphone, and it will periodically record sound if it recognizes someone speaking. The recordings you make as well as the random sampling of ambient sound are sent to the company that makes the app to improve their services and to third party advertisers. By paying for the app, you can prevent the app from recording ambient sound and from sending any data to third parties. The app will still continue to send data to the company for service improvement purposes.
4. Exercise *A*: Moderate *UC*: Moderate	You use an app to help you exercise better. One of the app features is a scoreboard that compares your performance with other app users. You can check out user profiles and see their individual scores, heart rate, and/or weight over time. You have the option of making your own profile private but doing so will prevent you from being added to the scoreboard.
5. Calendar *A*: High *UC*: High	You book a flight using your Google Mail as the contact email address. As you open your calendar to enter the flight information, you notice that it has already been added automatically. You find a feature in Google Mail that enables or disables this service.
6. Voting *A*: High *UC*: Low	You voted for a different political party for the first time in many years. You start to notice that the party for which you voted suddenly seems to have a far stronger presence on social media. Your friends claim that they barely see anything from that party online.
7. Photo *A*: High *UC*: Low	You uploaded a photo from a family dinner to your Facebook account. A month later, you come across an ad that uses your photo. You have no way of challenging the use of the photo in the ad.
8. Messenger *A*: High *UC*: Moderate	You have been arguing a bit more than usual with your significant other over Facebook messenger. Over time, you start noticing ads for couple counseling and dating. You can tell Facebook that these ads are inappropriate.

4 FINDINGS

Although the scenarios that we asked our participants to discuss were fictional, the conversations they spurred were connected to real-world mundane experiences with technology. We designed the scenarios to trigger concern and discomfort by violating commonly held expectations of data disclosure or confirming the negative data practices people might have imagined. It should not therefore be a surprise that a sense of discomfort with the use of technology was apparent in the interviews. Based on the literature, we expected this sense of discomfort to align with expressions of digital resignation [7, 25] and learned helplessness [88, 91]. We further identified a nested and paradoxical relationship between feeling empowered to control one's own privacy and a general resignation to the futility of attempts to manage privacy. Empowerment emerged as a limited and conditional experience arising against the backdrop of resigned fatalism regarding a creepy, invasive, and data-hungry technology culture.

The interviews reflected that participants had internalized notions of privacy rooted in self-determination and self-control. However, technology use in service of everyday practices does not conform to the neat lines laid down by the expectations of rational action and privacy calculus [67]. Yet, participants believed that they should be able to manage unwanted data disclosure because the necessary information is either implicitly or explicitly available via simplified EULAs, Terms of Service, Privacy Policies, etc. At the same time, many participants readily admitted to never having read the relevant information and expressed guilt for failing to do so. In the words of one participant, there is a "very fine line" between privacy maintenance and privacy violation.

Table 2: Demographics of the study participants.

Participant	Gender	Age	Occupation
A	Female	25	Student (Law)
B	Female	26	Web Designer
C	Female	27	Student (HCI)
D	Non-binary	21	Student (History)
E	Male	26	Writer
F	Male	29	Systems Analyst
G	Female	23	Student (Pharmacy)
H	Male	31	Student (Informatics)
I	Female	26	Business Analyst
J	Male	47	Call Support
K	Female	25	Student (HCI)
L	Male	30	Software Quality Assurance
M	Non-binary	30	Model
N	Male	36	Database Admin
O	Female	42	Court Clerk
P	Male	37	Sales Executive
Q	Female	36	Homemaker
R	Male	36	Package Handler
S	Female	46	Admin Assistant
T	Male	21	Student (Music Performance)
U	Male	21	Student (Information Systems)
V	Female	51	Professor (Chemistry)
W	Female	21	Student (Biology)
X	Female	21	Student (Biology)
Y	Female	27	Student (Biology)

In the following subsections, we first discuss participant rationalization of their privacy-related actions, the conditional empowerment experienced due to the impossibility of enacting privacy control, and the use of digital technologies despite privacy concerns and violations. We proceed to introduce the concept of *hyperbolic scaling*, which we define as a form of framing where specific and limited instances are generalized to an 'always' or 'everything' condition. We then explore the sense of resignation that is pervasive in the interview responses.

4.1 Rationalization

Privacy is nebulous, in part because in daily life it is more of practice than a concept, and practices are necessarily situated. Yet, the increased prevalence of the term 'privacy' in the news, media stories of data breaches, and frequent notifications requesting access to data serve to give this concept a practical meaning. Every day, people are asked to make privacy-management decisions when using digital technologies. When reflecting on these choices, people sometimes build elaborate rationalizations for choosing to give up privacy when they may be expected to protect it. As one participant put it:

> "A lot of the convenience that software tries to add to our lives is fueled by the data that we impart into the digital world. So there are definitely risks, but also benefits. It's a very fine line between your privacy or the invasion of your privacy being beneficial or malicious and risky." – Participant F (Male, 29, Systems Analyst)

Privacy cast as a "fine line" drives rationalization by serving as a justification for data-sharing demands that are rewarded by app-based benefits. Discomfort at having to walk this fine line when making disclosure decisions was ever present across the interviews, sometimes resulting in bewildering stories of technology use as exemplified by the practices of Participant B (Female, 26, Web Designer):

> Participant B: "I do have an Amazon Dot. But I feel uncomfortable like using it."
> Interviewer: "What is it?"
> Participant B: "Amazon Dot is like a speaker but it is always plugged in so it can basically record your conversations."
> Interviewer: "So you don't use it as often because…"
> Participant B: "Yeah, it's not plugged in at all. If I need to use it, it might be like while I'm cleaning my room, I will plug it in and turn it on and play music through it. But once I'm done, it's off and sitting in my closet."

In this case, Participant B rationalizes her use of the Amazon Dot despite her discomfort with its privacy-invasiveness. She describes mitigating the risk of using a data-hungry device by leaving it unplugged in her closet when it is not needed for its intended use as a mere music player. Thus, Participant B manages privacy by straddling the line between use and non-use.

The grey area around the fine line between beneficial and invasive disclosure can be fraught with uncertainty and feelings of guilt. In line with typical contemporary characterizations, people often view privacy as a personal choice. Echoing a common thread among the participants, Participant H noted:

> "I still would probably use [the app]. But it'll probably always be in my mind kind of a guilty pleasure like listening to a boy band … you don't tell that to anybody." – Participant H (Male, 31, Student [Informatics])

The performance of responsible technology use that underlies end-user privacy management is akin to lofty yet difficult-to-achieve self-improvement goals, such as regular exercise. Privacy is a boulder, and privacy management is a Sisyphean task [87]. In the act of climbing the mountain boulder-at-hand, participants reported encountering trade-offs related to the context of daily life. Across scenarios, participants mentioned trades-off between privacy and competing forms of discomfort. The technologies that necessitated considerations of privacy violations were also the technologies that provided benefits (or guilty pleasures). Participants rationalized tolerating the potential invasions of privacy by pointing to the benefits of the technology. Participant Y justified the use of a hypothetical application (Scenario 3) that provides voice-based user interaction and uses ambient listening to improve transcription:

> "The pros of the service that they're giving far outweigh my invasion. Focusing on the hardware, this does improve service." – Participant Y (Female, 27, Student [Biology])

Yet, many participants set the benefits of digital technologies against a backdrop of discomfort that emerges out of the ambiguity of the intrusion. Not only are privacy violations ambiguous, but so are the motivations for anxiety over potential privacy violations.

The tendency of the participant to offer rationalizations for their practices underscores that they accept individual responsibility for personal privacy management, understanding it as an uncertain and generally uncomfortable process of balancing practical trade-offs. Curiously, participants could not clearly delineate the contours of the trade-offs beyond the obvious high-level characterization of the benefits and conveniences versus an uneasy feeling regarding handling of their personal data. Participant E highlighted these tensions:

> "So privacy to me is just my general right to keep to myself, my right to keep any information about me private. At the same time, I believe there are certain trade-offs that come with privacy, and there are things to be gained when you're willing to, I wouldn't say sacrifice, your privacy, but I think the word I'm looking for would be more like a social contract, where I give a bit of my privacy for optimized music choices . . . So privacy to me isn't what's really important. However, I do in some ways view it kind of as a social currency that we exchange in return for features or functions." – Participant E (Male, 26, Writer)

Participant E attempted to define privacy as the right to keep personal information private. Although somewhat tautological, this is a common definition underlying much privacy research. Privacy is treated as variable that the user must negotiate with the parties that demand data to provide benefits. Yet, our findings suggest that rather than understanding privacy as cost-benefit calculations, it may be more productive to think of privacy practices as rationalizations, tinged with guilt and discomfort and fostered by constant trade-offs.

4.2 Conditional Empowerment

In today's digital world, people live their lives through and by means of technology. Ideally, technological empowerment should manifest as the *power to* control the conditions of one's life or at least one's ability to get things done. In a broad sense, technology can be empowering if it enables users to achieve what they were not previously able to do, perhaps even enhancing their capacity to have a better life. However, as discussed in the previous subsection, the use of digital technologies is increasingly a balance between the *power to* obtain benefits and avoid the disclosure of personal data. The enforcement of data disclosure as a condition of obtaining the benefits of technology use necessitates accepting that the parties that design the technologies have *power over* the user through and by means of data.

When use of a technology is deeply embedded in everyday life (e.g., Facebook, Google, etc.), users must accept the *power over* that these technologies have in demanding particular data exchange relationships. The technologies may empower users to do things they couldn't do before, but such *power to* is contextualized entirely by the *power over* personal data of the users. Such empowerment is deceptive because it is conditional. The *power to* becomes 'the power to do what the user is allowed to do':

> "I'm familiar with the service. I've used it, I love it. It's so convenient. It's highly intrusive. I already know that. But Google already knows everything. It's what I signed up for. It's what I'm aware of. It's in my own hands." – Participant P (Male, 37, Sales Executive)

Theoretically, people can choose to delete an app or deactivate an account. Indeed, if a technology creates a sufficiently high level of discomfort, people can and probably will stop using it:

> "I usually test it out by myself. I download it and then see if I like it. If not, I just delete it." – Participant U (Male, 21, Student [Information Systems])

However, not using certain technologies can lead to disconnection from the social environment, making it difficult, if not impossible, to consider quitting the use of the technology in question. In such cases, participants tended to downplay the privacy intrusion and accentuate the value. Speaking of Scenario 7 (Photo), in which a photo posted to Facebook shows up (unauthorized) in an advertisement, Participant E exemplifies this tendency:

> "It's definitely a negative scenario. No one wants to see that kind of thing happen. But, at the end of the day, I don't think it outweighs all the positives that Facebook brings to the table, for me at least." – Participant E (Male, 26, Writer)

Focusing on the benefits does not mean that people are not bothered by the accompanying privacy violations. In fact, our data is rife with examples of anger and frustration at the inability to take action against apps or platforms for causing discomfort through the privacy trade-offs they demand:

> "But for [Facebook] to say, 'hey, we've taken this' . . . I'm sure this might be one of those [things] in the TOS [Terms of Service]. So there's no recourse and if it was the case that it was in the TOS, I'd be like, 'Honestly, screw you guys! I can't do anything about challenging you guys.' [. . .] If it was one of those [things] hidden in legalese . . . but no one reads the TOS. Being honest, no one does that. So it's like that expectation of 'Well, you should!' Yeah, me and my team of high-priced lawyers? . . . me making $30,000 a year? No, that doesn't happen!" – Participant N (Male, 36, Database Administrator)

For most people, the *power to* use or not use a technology is entirely contextual and comes with its own cost-benefit calculations. This context includes available alternatives, existing pressures and needs, and the fulfillment of relational obligations [90, 106]. The calculus involves not merely trading personal data for benefits, but a much more complex and multi-faceted set of considerations. For instance, when presented with Scenario 4 (Exercise), a fitness app that offers social comparison features as a benefit for data disclosure, many participants found it relatively easy to deny data access:

> "I don't really like that feature of the scoreboard thing. Because exercising and being healthy is a really personal thing. It's not good if you focus on other people and what they're doing because your journey is different. Everybody does things differently, and that'll just turn that into a game for some people, when health is not really a game to me." – Participant T (Male, 21, Student [Music Performance])

In contrast, when it comes to negotiating and balancing the needs of others, wanting to quit universally-adopted services is deemed impossible:

> "My church isn't that great about emailing. So how do I know what's going on if they're not sending email? It just seems like Facebook is the natural feed for all things related to people's messages that are not personalized." – Participant S (Female, 21, Student [Biology])

The *power to* stop using a one-off app or a certain feature of a technology is always present, but exercising this power is less realistic when it comes to technologies that are deeply embedded within social and economic infrastructures. For example, Google, Facebook, and Amazon are not just services, but an integral part of participation in societal transactions. To be empowered to act within the parameters imposed by the entities that control the dominant technologies, without recourse to their demands, is not to be empowered at all.

4.3 Reluctant Use

Conditional empowerment is insidious because it masquerades as general form of *power to*. The person who uses a technology is conditionally empowered by becoming the 'user,' but the condition of being a user is often creepy and uncomfortable. In a culture in which data-hungry technologies are pervasive, it is becoming increasingly difficult to remember or envision a world where the ubiquitous trade-off that is the contemporary discourse of privacy was not omnipresent. Instead of fighting these larger trends in technological developments, participants reported resorting to adopting them, albeit reluctantly:

> "I think [apps make] things more convenient, and it's easy to be become a little bit dependent on them to track everything. But it does make life easier." – Participant V (Female, 51, Professor [Chemistry])

As everyday life is increasingly experienced through the digital filters and feedback loops of various technologies, conditional empowerment might appear as a form of *power to* control one's life. As new features of technology become ever more invasive, people can encounter further conditional empowerment, finding ways to rationalize the discomfort and creepiness that underlies their reluctant use:

> "I remember back when tagging became a thing, people were like, 'Whoa, this is creepy, this is weird.' But I think what ended up happening was I think it was just kind of fair knowledge that by the subtle uses of features in the platform, it was very obvious that they were using photos." – Participant K (Female, 25, Student [Human-Computer Interaction])

Participants frequently described feelings of creepiness and discomfort when discussing their reactions to the various scenarios. Despite the clearly negative valence of these affective experiences, participants worked to explain their reluctant use:

> "I feel like this is a pretty common thing. I guess it is sometimes a little creepy. Things like this happen a lot on Google, right? Where if you search for something, especially if you're online shopping, that thing will pop up across your social media or across your google searches. I think it's the price you pay for using these free technologies." – Participant W (Female, 21, Student [Biology])

In fact, creepiness is pervasive enough to belong to its own category of user experiences, as illustrated Participant P's use of the phrase "one of those" when describing such an experience:

> "This is one of those creepy moments where my spouse and I were just sitting around talking about shoes, like Nike shoes, and then I pick up my phone and go to Google – we were going to order food or something – and all of a sudden a shoe ad pops up. What the heck?!" – Participant P (Male, 37, Sales Executive)

While creepy experiences are unwelcome and invasive, they are often not negative enough to warrant strong repudiation. Facebook, for example, seems to have acquired creepiness as an inherent expectation of use:

> "I feel like this is also a bit creepy, but it's not surprising considering it's Facebook." – Participant W (Female, 21, Student [Biology])

Such passive acceptance of creepiness reflects resignation regarding the use of digital technologies. Acknowledging that benefits of technologies require the cost of data disclosure necessitates reluctantly accepting feelings of creepiness when using these technologies.

4.4 Hyperbolic Scaling

Participants rarely mentioned attempts to manage privacy beyond decisions of use or non-use, despite the plethora of other available privacy solutions. In part, such a broad view had to do with their perceptions of the scale of the data economy and the uncertainty regarding the parties involved in collecting and using their data:

> "Because of the ubiquity of computing, it's kind of inevitable that someone will have access to some of your data at some point." – Participant F (Male, 29, Systems Analyst)

Most participants believed that data disclosure is inevitable and felt that the range of actors included in the category of "someone," whose access to data is unwelcome, but unavoidable, is broad and heterogeneous:

> "They're like that third-party that knows what I'm doing." – Participant I (Female, 26, Business Analyst)

Notably, the use of "that" in the quote above represents the knowable but unidentifiable "they" and "someone" that pervades interview discussions. In its simultaneous definiteness and lack of specificity, "that" indicates a general awareness of the category of the third party but uncertainty regarding the heterogeneous actors who populate that category.

However, the vague references to third parties did not stem from a poor understanding of the parties and mechanisms involved in the maintenance or production of privacy. On the contrary, it demonstrates a worrying form of adapted understanding: there is always someone who will gain unwanted access to personal data. The unidentified third party was a known, if unidentifiable, factor in

daily experiences with privacy decisions narrated by participants. For most participants, the clearest indicator of the presence of third parties was personalized advertising embedded within the technologies they used. Even as the recognition of the ambiguous category of third parties demonstrates a general understanding of privacy as a trade-off, it lends itself to an overall wariness. When one app gave participants reason to believe that hidden third parties are involved, they tended to generalize that property to all apps. We refer to this tendency as *hyperbolic scaling*: a form of framing where specific and limited instances are generalized to an 'always' or 'everything' condition.

When discussing specific applications and the extent to which they 'know' things about the user, participants made routine and frequent use of hyperbolic scaling. In the logic of hyperbolic scaling, if App X demonstrates Property A, then Property A is assumed to be a likely property of all apps. For instance, as a consequence of hyperbolic scaling, the problematic characteristics of one app or a small subset of apps are attached to the entire category of apps. Hyperbolic scaling is thus a form of inference in which users base judgments regarding a given general technology on their observations and experiences with one or few specific examples of that technology:

> "Because all those [apps] connect, just like with that one previous situation of music and the top weekly chart, it's the same thing. It's a combination of everything you do online or on that platform." – Participant T (Male, 21, Student [Music Performance])

When "all those apps connect," an app is not just an app. The perceived interconnection of apps forms an infrastructure that is both real and imagined: an emergent sociotechnical system that is characterized by the ubiquity of apps and data collection. For Participant T, the *power to* is contextualized and mitigated by sheer numbers: "a combination of everything you do online, or on that platform." The *power to* manage privacy occurs within the context of *power over* the user as understood in terms of the folk theory that describes an app's relation to other apps, platforms, and parties. When one app demonstrates *power over* the user in a creepy or intrusive way, it serves as an archetype for apps in general. This is apparent in participant use of canonical examples, generally drawn from news stories. When speaking of their concern for privacy, participants rapidly hyperbolically scaled specific small-scale intrusions to the scale of the vast and infrastructural:

> "It kind of reminds me of the problems they had at one point in time with Amazon Echo where they're recording everything. It seems like that could be an issue, especially since they're sending this information to advertisers. I don't like that, so I would not want to use it." – Participant O (Female, 42, Court Clerk)

The totality of "everything" as used above to refer to information cannot be read literally. Yet, it is the most common way of describing the extent of knowledge about the user. The imagined infrastructure that emerges from the logic of hyperbolic scaling can be vast.

The discursive transformation of hyperbolic scaling can lead to a fatalism about privacy. Users come to believe that their personal data cannot and will not remain private, no matter what they do:

> "I don't think it's gonna really matter because either way they're probably gonna find out about it so I don't think it really matters." – Participant R (Male, 36, Package Handler)

4.5 Empowering Resignation

Participants understood clearly that empowerment through technology is typically associated with costs. At the same time, their views reflected a general perception that disclosure of personal data to various known and unknown entities is undesirable, and they bear the responsibility of making appropriate decisions to manage data disclosure. However, fulfilling this responsibility for privacy management is practically impossible owing to the scale of the problem and the limits of individual agency, conditional as it is on one's capacity to act within the possibilities and constraints of various limits, demands, and obligations. For example, participant responses to Scenario 7 (Photo) typically expressed that the use of a family dinner photo in an advertisement was wrong yet indicated resignation to the inevitability of such a violation. The conflicting perspective is captured in the reaction of Participant A (Female, 25, Student [Law]):

> Interviewer: "What do you think about the option to tell Facebook that it's inappropriate?"
> Participant A: "The ad will go away, but I don't think that will stop anything like it and won't prevent the practice of getting information from messaging in order to target your advertisement. So it feels like this one ad will go away, but I don't think it will stop the actual root of the problem."

Even if the individual's *power to* deny a specific disclosure is enabled by the functionality of the system, it remains inadequate. The root of a system's *power over* is not just in how it structures and limits individual capacity to decide what to disclose, but also in how that system is socially and relationally embedded in different aspects of life. For example, such *power over* led participant A to continue using Facebook despite being uncomfortable with its handling of her data:

> "I think it's just because everyone has Facebook, and I feel like I use Facebook Messenger with my classmates more. Rather than having to exchange Facebook and phone number, it's easier to exchange Facebook and just use Facebook Messenger because it's essentially just as easy as texting. So it's an easier way to connect with people whom I'm not closest to but still keep in contact with." – Participant A (Female, 25, Student [Law])

People do not have a clear or easy way of addressing the causes of creepiness or discomfort with the assemblage of people and institutions behind the digital technologies they use. This is particularly difficult when the technologies are socially infrastructural:

> "I feel [Facebook has] kind of made themselves into a service where it's just very convenient to use them for a lot of things. I thought about deleting Facebook once. But I was just like, 'Oh, I don't think I would delete' because people will send me event request,

> right? They'll tell you something's going on or you can see people's life updates. I feel like it'd be kind of sad to miss out on that. So I'm okay with dealing with some of these more shady things to have what I get out of that service." – Participant W (Female, 21, Student [biology])

As people encounter privacy issues across nearly all socially infrastructural digital technologies, they resign themselves to experience discomfort as an essential affective facet of privacy-related user experience. Interestingly, the desire to limit the discomfort can lead people to adopt solutions within the same technological ecosystem, further solidifying the ecosystem's *power over* constraining their *power to* enact their privacy choices. For instance, participants reported using multiple apps and services of a single provider, such as Apple or Google, as they presumed that data would be shared across all offerings of the provider. By sticking to a single provider, participants hoped to constrain their uncomfortable data disclosures within a single ecosystem. The *power over* of a system can thus permeate into more and more facets of a person's life. The system conditionally empowers users with enhanced capabilities. However, loyalty to the system, and implicitly its privacy-related ethics, is the condition upon which the system's end-user benefits are predicated. As a result, the capacity of users is limited by the system's *power over* them:

> "I know that when you sign up for a thing and click the little box of terms and conditions, that's it. If you agreed to use a service and part of their terms is that you give up your photos to the company so that they can do what they want with them, then that's that. So I feel like it's more a sad reality of what we've decided to accept and allow companies to do. I think it's a larger issue rather than 'Oh, I need to fix this for myself.' I think that this is a symptom of social media in 2020." – Participant A (Female, 25, Student [Law])

Such contractual agreement demonstrates the hierarchy of *power over* as it relates to the *power to* and serves as the foundation that gives rise to resignation:

> "You just don't see it, but [Facebook] still [has] that information about you. It's not like once you're like, 'Please don't show me these ads,' they delete the information they have about you. So I don't know. They already have it at that point, so you can't really do much about it." – Participant W (Female, 21, Student [Biology])

When the system's *power over* outweighs the user's *power to*, users face difficult choices predicated on an awareness of unidentified third parties gaining access to their data. When making typically uncomfortable decisions based on such fuzzy privacy calculus, people generally perceive little power to mitigate negative privacy-related experiences:

> "I think if it was in their Terms and Conditions beforehand, they probably wouldn't do anything. You probably wouldn't have much legal power over them anyway. So I just feel like this is kind of a lost cause." – Participant W (Female, 21, Student [Biology])

Participants frequently expressed such sentiment going so far as to surmise that having no recourse to protest a feature must indicate that they consented to it:

> "If there's no way to challenge it that means it was part of the privacy policy I agreed to." – Participant B (Female, 26, Web Designer)

Several participants went a step further and exhibited the tendency to blame themselves based on perceptions regarding typically expected privacy-related practices [61]:

> "I'd feel kind of defeated and cheated, and I imagine the fact that this happened means there's something in the fine print that I didn't account for that led to me not being able to challenge this." – Participant F (Male, 29, Systems Analyst)

People judge themselves and others based on the ability to be responsible regarding data disclosure. Individual *power to* make decisions about which technology to use and what data to disclose might be clearly conditional and constrained within layers *power over* of other actants, but the sense of personal responsibility remains regardless:

> "Privacy is always a concern with people online . . . whether it's on their phone, laptop, whatever way information is easily accessible to others. This is interesting to me because, as a consumer, I can choose whether to use an app. That company can decide what they do with my information if I'm using that app. So to me this is a little bit non-negotiable. When people are like, 'Oh, I got hacked. They did this. they did that,' they are really quick to point the finger at privacy issues when it comes to using websites or apps. It's a free-for-all if you're going to put your information out there. Expect for it to be used." – Participant S (Female, 46, Administrative Assistant)

In the folk theories they construct in order to understand what's going on, people assign fault to themselves even if they are the ones who feel "defeated and cheated." Participant S went so far as to blame the victim for failing to recognize the nature of the power structure between users and technology. Our findings highlight that people internalized the responsibility for managing their data yet they fail to do so and cannot therefore complain when things go awry. The practical impossibility of the performance of responsibility results in further resignation.

5 DISCUSSION

Privacy continues to be a contested concept. The mechanisms for privacy protection are political decisions with real consequences no matter how technical they appear [61]. Power is not evenly distributed across actants enmeshed in the network constituted by the user-app-device assemblage. Our findings point to fundamental issues around data infrastructures and platform relations that impact user capacity to make privacy choices despite the intentions of app developers. A focus on individuals and their decisions with respect to a specific device or service may circumscribe and clarify the privacy-related problems to be solved by providing better information or simpler choices, but such a focus ignores the different

kinds of *power over* that define whatever *power to* is possible to protect individual privacy.

Within these power structures, the insistence on individuals addressing their own privacy concerns is normative. When power structures or their perceptions are in flux, creepiness emerges as a symptom of a mismatch between normative expectations and technological capabilities [23]. Notably, the expected social contract underlying the obligations and responsibilities engendered by technology use is never quite defined. The *power over*/*power to* framework for thinking about what it might mean to empower people to use technology and assert control over their data offers a way to reconsider the usual approaches. Our framework challenges and complicates core notions of the privacy debate, such as the privacy paradox, informational self-determination, and end-user responsibility. By placing *power over* and *power to* as conceptually central in the analysis of user experience *vis-à-vis* privacy, we see a productive opportunity to challenge, and perhaps displace, the primary rhetoric of an approach to user empowerment that is, in effect, disempowering.

5.1 The Problem of the Privacy Paradox

The privacy paradox is a common refrain in the privacy literature. It is the lament that people routinely engage in actions that do not match their stated valuations of privacy [72], essentially saying one thing while doing another. As Hanson et al. [36] neatly summarize: "A common explanation for this paradox is that people engage in privacy calculus, weighing privacy risks against perceived benefits." Such commodity-based foundations of the privacy paradox [54] situate it in as pragmatic calculation that places high value on rational action. Yet, strict rationality is not always an appropriate lens through which to view human action [92], which is bounded and contextual. Our lens of *power over* and *power to* suggests a different interpretation of the privacy paradox. Matters seem less paradoxical if the conditions of power that are invoked when *valuing* privacy are different from those that are invoked when *enacting* technology use and balancing the conflicting contextual possibilities and demands.

The unrealistic expectation of achieving privacy is aspirational and hopeful, thus making the valuation of privacy a kind of idealization. It represents a process by which the user envisions a balance in the system of *power over* and *power to* that is acceptable as well as manageable. People know that privacy is important; stories, news coverage, pop-up notifications, and EULAs tell them so. The difficulties of privacy control do not reside in specific apps or users, but in the systemic power relationships that characterize them. High valuations of privacy likely allude to a set of aspirational power relationships that a person envisions. The enactment of privacy concerns in a manner that does not match high valuations suggests a resignation to the pipe dream of privacy in reality.

In contrast to the hypothetical and aspirational nature of valuations, actions are situated and bounded by conditional empowerment: the specifics of a user's relationship with a given technology as defined by a distribution of *power over* and *power to*. The manifestation of a user's *power to* is not subject to purely rational assessments of the world, but to folk explanations or beliefs such as hyperbolic scaling. Action thus happens in a reality constrained by conditional empowerment and the heuristics used to make sense of fundamental power imbalances. These constraints may account for the discrepancy between privacy valuation and enactment.

The privacy paradox ceases to be paradoxical if we recognize that there is a fundamental mismatch between the aspirational conditions under which people value privacy and the real-world context in which they make privacy-related choices. When we take power into account, the privacy paradox surfaces a deep-rooted flaw: systemic inequalities in the power distributions that characterize the relationships between the user and the other actants involved in the ecology of digital technologies. These systemic issues lead to digital resignation and privacy fatalism as people internalize privacy management as their own responsibility, despite such control being unattainable.

5.2 The Folly of Individual Control over Data

The idea that privacy is an individual problem underlies everything from the design of privacy settings to policy solutions. Much privacy discourse is dominated by Westin's [109] description of privacy as "the right of the individual to decide what information about himself should be communicated to others and under what circumstances." Yet, this conceptualization of privacy as requiring self-management is a form of atomized isolation that limits the possibility of collective action. As Draper and Turow [25] put it, "the heart of the problem relates to corporate efforts aimed at disempowering the collective while keeping the focus on the individual." This focus on individual choice with respect to privacy is particularly problematic if we consider PETs and other efforts to support users. As Stanton et al. [98] have shown, the provision of end-user responsibility for security can ultimately lead to security fatigue and negative affect, including "resignation, loss of control, fatalism, risk minimization, and decision avoidance."

Participants in our study judged the data disclosure decisions of themselves and of other's around them by casting them as individual actions, never referring to them as matters for collective achievement. When privacy-related decisions are seen as personal choices, failures to achieve the ideal of responsible data disclosure becomes akin to failures to eat healthier despite vowing to lose weight. When discussing data misuse, participants blamed themselves and their friends for actions such as succumbing to conveniences and guilty pleasures, despite knowing that the technologies are problematic in terms of privacy. Holding everyone personally responsible for their actions discourages any form of collective action. Yet, as an individual, it is practically impossible to perform what it takes to enact the professed concern about privacy.

Westin's [109] conception of the individual deciding to disclose information hinges on the person having at least a vague understanding of the audience for this disclosure and perhaps even the reasons behind it. While participants in our study were clearly aware of the presence of third parties in most data transactions, such parties were vague unknowns hidden in the shadows beyond their screens. This lack of visibility is one of the sources of the discomfort many people experience when using technologies. After all, it is creepy if you know that someone else is always watching, but you can never really know who or why. We do not mean to

imply that this deception is wholly intentional, although there is evidence to that it might be partially true [104].

Privacy decisions are rarely one-off decisions regarding whether to allow access to a particular piece of data. Instead, the disclosures are embedded in many different demands, obligations, and responsibilities. The *power to* decide about disclosure is always defined and circumscribed by the *power over* exercised by platforms setting non-negotiable constraints, employers decreeing particular apps for particular tasks, and even personal social networks where choices of what to use for communication define who can participate and how [106]. The situation is further complicated by the lack of clarity regarding the specific obligations and responsibilities that underly interactions with a given platform, service, or app. The social contract of expectations for appropriate behavior is under-defined. The structural conditions and situational opportunities and constraints of people's lives are continually reshaped by the technologies we build. As a result, individuals must constantly renegotiate their contract with the social structures they inhabit.

To make progress in supporting people in managing privacy as they face data-hungry digital technologies, it is important to acknowledge that making minute data disclosure decisions by responding to a continuous stream of settings dialogs, notifications, nudges, etc., places a too great a cognitive burden on users. To make matters worse, people's individual decisions have an impact beyond themselves because people live in the complex and interwoven networks of society. People might want to act in their own best interest, but the impact of those actions on the interests of others must be considered as well. Privacy researchers and developers of PETs need to recognize that decision-making capacity is never evenly or fairly distributed [61, 74]. *Power to* make decisions is contingent on the privilege of having *power over* data demands. Designers must not assume that users have the *power to* make decisions without reflecting on the privilege the decision-making necessarily requires.

5.3 The Limits of Responsibility

Contemporary problems of privacy and data disclosure arise in part because of the way technical infrastructures have been, and continue to be, built. Privacy concerns were debated as a set of logistical problems at the inception of the Internet, and the decisions made then have resulted in today's data infrastructures [14]. Infrastructures empower and constrain what is possible within their confines. For example, the privacy protection of message encryption is limited by the information revealed by metadata. There is considerable agreement across domains that the current data extraction and exchange infrastructures are problematic. While characterizations of the nature of the problem vary, there is some agreement that individuals must take responsibility for their digital data activities. Researchers have stepped in by developing various solutions to support users in taking responsibility [24]. Despite the availability of such solutions, users continue to 'misbehave,' disregarding EULAs, using leaky apps, ignoring security updates, and so on. However, these user practices should not be taken as a sign of users being irresponsible. "Inaction is a rational response to a seemingly inevitable outcome" [25], especially in situations where individuals hold little power. As our findings demonstrate, people have internalized a sense of personal responsibility for their data disclosure despite the difficulties in achieving real control over privacy. As a consequence, people engage in practices that they think may help even though they acknowledge the likely futility of these practices.

Sociotechnical systems and the networked, interconnected nature of life challenge notions of responsibility in interesting ways. Yet, current solutions typically ignore people's sociotechnical entanglements, typically presuming that each privacy-related decision happens separately from others. People must make a never-ending series of such decisions when installing, configuring, using, and updating digital technologies, while attempting to maintain ecological consistency. If users are continually presented with information in a growing range of formats at increasingly finer granularity, it should be no wonder that they exhibit fatigue and learned helplessness [7, 91], eventually resigning to their fate. Privacy solutions based on individual user control simply add responsibility under impossible conditions, thus empowering resignation.

Simon [93] argues for distributed responsibility: "within our practices of knowing, we depend upon other human and nonhuman agents just as much as these other agents depend on us." Individuals can not be responsible for all of the necessary data decisions by themselves, but perhaps they can achieve more together. This idea has manifested in arguments for data commons and data cooperatives, unionization proposals, and community data networks[1] [19, 64]. These solutions attempt to change the conditions of *power over* that define the power of the individual to make decisions regarding data. While efforts to automate and personalize privacy-related decisions [55] are useful, a complimentary orientation might be to design mechanisms for grassroots organizing around the privacy misbehavior of apps or services, providing functionality for collecting evidence of undesirable data practices that can serve to inform the entire user community and induce collective action.

Although it is tempting to frame the further development of such an orientation as an 'implication for design,' we actively avoid doing so. As we see them through the words of the participants, the problems of privacy and empowerment cannot be designed around or mitigated simply by designing a better app or platform. In developing technical solutions it is important to always keep in mind that giving users a form of *power to* may not be enough because such empowerment is bound up in the dysfunctional current systems of *power over* manifest in surveillance capitalism [117]. Therefore, we call on system designers, researchers, and policy makers to consider the possibilities of users possessing and exercising *power over* the data infrastructures underlying the devices, platforms, services, and apps they routinely use.

6 LIMITATIONS

As with most qualitative studies, our sample is relatively small. Moreover, our insight is derived from self-reports of relatively young participants from the United States. Larger and more diverse samples from other populations have the potential to illuminate important cultural differences and verify generalizability.

[1] See also: http://orkneycloud.org

7 CONCLUSION

The conceptual and practical framing of privacy that ostensibly empowers users by placing the responsibility for privacy maintenance on them is ineffectual and counterproductive. For users, privacy exists not as a concept or a set of actions toward a solution, but as a quagmire of trade-offs between bad and worse options that contributes to a fatalistic sense of resignation. Given the pervasiveness of such resignation and evidence to support its relationship to affective experience, we contend that it is time to rethink such canonical phenomena as the privacy paradox through the lens of power relations and give serious consideration to the affective, power based, and relational aspects of privacy matters related to digital technologies.

ACKNOWLEDGMENTS

We thank the participants of study. We are grateful to Nanna Gorm and Malik Kreutzfeldt for ideation and scenario development, and James Theesfeld for updating the scenarios and collecting the pilot data. We acknowledge Emma Lashley and Emily Swiatek for helping transcribe the interviews.

REFERENCES

[1] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce* (Denver, Colorado, USA) *(EC '99)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/336992.336995

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[4] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.

[5] Idris Adjerid, Alessandro Acquisti, and George Loewenstein. 2019. Choice architecture, framing, and cascaded privacy choices. *Management Science* 65, 5 (2019), 2267–2290.

[6] Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company, Pacific Grove, CA.

[7] Mark Andrejevic. 2014. Big data, big questions: The big data divide. *International Journal of Communication* 8, 6 (2014), 1673–1689. https://ijoc.org/index.php/ijoc/article/view/2161

[8] Hannah Arendt. 2013. *The human condition*. University of Chicago Press.

[9] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[10] Sara Bannerman. 2019. Relational privacy and the networked governance of the self. *Information, Communication & Society* 22, 14 (2019), 2187–2202.

[11] Jeffrey Bardzell, Shaowen Bardzell, Amanda Lazar, and Norman Makoto Su. 2019. (Re-)framing menopause experiences for HCI and design. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300345

[12] Louise Barkhuus. 2012. The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 367–376. https://doi.org/10.1145/2207676.2207727

[13] Steve Benford, Chris Greenhalgh, Gabriella Giannachi, Brendan Walker, Joe Marshall, and Tom Rodden. 2012. Uncomfortable Interactions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 2005–2014. https://doi.org/10.1145/2207676.2208347

[14] Sandra Braman. 2012. Privacy by design: Networked computing, 1969–1979. *New Media & Society* 14, 5 (2012), 798–814.

[15] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347.

[16] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2018. Thematic Analysis. In *Handbook of Research Methods in Health Social Sciences*, Pranee Liamputtong (Ed.). Springer Singapore, Singapore, 1–18.

[17] Alex Braunstein, Laura Granka, and Jessica Staddon. 2011. Indirect content privacy surveys: Measuring privacy without asking about it. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 15, 14 pages. https://doi.org/10.1145/2078827.2078847

[18] Fred H. Cate. 2010. The limits of notice and choice. *IEEE Security & Privacy* 8, 2 (2010), 59–62.

[19] Niels Ørbæk Chemnitz, Philippe Bonnet, Irina Shklovski, Sebastian Büttrich, and Laura Watts. 2020. Unionized data governance in virtual power plants. arXiv 2006.02709.

[20] Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, and Yuvraj Agarwal. 2017. Does this app really need my location? Context-aware privacy management for smartphones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 42 (Sept. 2017), 22 pages. https://doi.org/10.1145/3132029

[21] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'privacy' for a networked world. *Computer Supported Cooperative Work (CSCW)* 26, 4-6 (2017), 453–488.

[22] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[23] Richard Cumbley and Peter Church. 2013. Is "big data" creepy? *Computer Law & Security Review* 29, 5 (2013), 601–609.

[24] George Danezis and Seda Gürses. 2010. A critical review of 10 years of privacy technology. *Proceedings of surveillance cultures: a global surveillance society* (2010), 1–16.

[25] Nora A. Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (2019), 1824–1839.

[26] Nico Ebert, Kurt Alexander Ackermann, and Peter Heinrich. 2020. Does context in privacy communication really matter? — A survey on consumer concerns and preferences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3313831.3376575

[27] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[28] Ricard L. Fogues, Pradeep K. Murukannaiah, Jose M. Such, and Munindar P. Singh. 2017. Sharing Policies in Multiuser Privacy Scenarios: Incorporating Context, Preferences, and Arguments in Decision Making. *ACM Trans. Comput.-Hum. Interact.* 24, 1, Article 5 (March 2017), 29 pages. https://doi.org/10.1145/3038920

[29] Steven Furnell and Kerry-Lynn Thomson. 2009. Recognising and addressing 'security fatigue'. *Computer Fraud & Security* 2009, 11 (2009), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

[30] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376651

[31] Barney G. Glaser, Anselm L. Strauss, and Elizabeth Strutzel. 1968. The discovery of grounded theory; strategies for qualitative research. *Nursing research* 17, 4 (1968), 364.

[32] Nathaniel Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan. 2005. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '05)*. Association for Computing Machinery, New York, NY, USA, 43–52. https://doi.org/10.1145/1073001.1073006

[33] Kevin D. Haggerty and Richard V. Ericson. 2000. The surveillant assemblage. *The British Journal of Sociology* 51, 4 (2000), 605–622.

[34] Foad Hamidi, Morgan Klaus Scheuerman, and Stacy M. Branham. 2018. Gender recognition or gender reductionism? The social implications of embedded gender recognition systems. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173582

[35] Julie M. Haney and Wayne G. Lutters. 2018. "It's scary...it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security.

In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 411–425.

[36] Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. Taking data out of context to hyper-personalize ads: Crowdworkers' privacy perceptions and decisions to disclose private information. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376415

[37] Woodrow Hartzog. 2018. *Privacy's blueprint: The battle to control the design of new technologies.* Harvard University Press, Cambridge, MA.

[38] Christine Hine. 1998. Privacy in the marketplace. *The Information Society* 14, 4 (1998), 253–262.

[39] Nis Johannsen and Finn Kensing. 2005. Empowerment reconsidered. In *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility* (Aarhus, Denmark) *(CC '05)*. Association for Computing Machinery, New York, NY, USA, 203–206. https://doi.org/10.1145/1094562.1094599

[40] Nicholas A John and Benjamin Peters. 2017. Why privacy keeps dying: the trouble with talk about the end of privacy. *Information, Communication & Society* 20, 2 (2017), 284–298.

[41] Yoonhyuk Jung and Jonghwa Park. 2018. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management* 43 (2018), 15–24.

[42] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. 2015. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* 25, 6 (2015), 607–635. https://doi.org/10.1111/isj.12062

[43] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: Installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, Bonaire, 68–79.

[44] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[45] Vera Khovanskaya, Eric P. S. Baumer, Dan Cosley, Stephen Voida, and Geri Gay. 2013. "Everybody knows what you're doing": A critical design approach to personal Informatics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3403–3412. https://doi.org/10.1145/2470654.2466467

[46] Jennifer King, Airi Lampinen, and Alex Smolen. 2011. Privacy: Is there an app for that?. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 12, 20 pages. https://doi.org/10.1145/2078827.2078843

[47] Agnieszka Kitkowska, Yefim Shulman, Leonardo A. Martucci, and Erik Wästlund. 2020. Facilitating Privacy Attitudes and Behaviors with Affective Visual Design. In *ICT Systems Security and Privacy Protection*, Marko Hölbl, Kai Rannenberg, and Tatjana Welzer (Eds.). Springer International Publishing, Cham, 109–123.

[48] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, virtual, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[49] Oksana Kulyk, Paul Gerber, Karola Marky, Christopher Beckmann, and Melanie Volkamer. 2019. Does this app respect my privacy? Design and evaluation of information materials supporting privacy-related decisions of smartphone users. In *Workshop on usable security (USEC '19)*. San Diego, CA, 1–10.

[50] James Laidlaw. 2010. *Agency and responsibility: Perhaps you can have too much of a good thing.* Fordham University Press New York, New York, 143–164.

[51] Markus Langer and Cornelius J König. 2018. Introducing and testing the creepiness of situation scale (CRoSS). *Frontiers in Psychology* 9 (2018), 2220.

[52] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[53] N. Pontus Leander, Tanya L. Chartrand, and John A. Bargh. 2012. You give me the chills: Embodied reactions to inappropriate amounts of behavioral mimicry. *Psychological Science* 23, 7 (2012), 772–779.

[54] Han Li, Xin Robert Luo, Jie Zhang, and Heng Xu. 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management* 54, 8 (2017), 1012–1022.

[55] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 27–41. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu

[56] Miguel Malheiros, Charlene Jennett, Snehalee Patel, Sacha Brostoff, and Martina Angela Sasse. 2012. Too Close for Comfort: A Study of the Effectiveness and Acceptability of Rich-Media Personalized Advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 579–588. https://doi.org/10.1145/2207676.2207758

[57] Stephen T. Margulis. 2003. Privacy as a social issue and behavioral concept. *Journal of Social Issues* 59, 2 (2003), 243–261.

[58] Kirsten Martin and Katie Shilton. 2016. Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society* 32, 3 (2016), 200–216.

[59] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. 2020. Exploring nudge designs to help adolescent SNS users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3313831.3376666

[60] Francis T. McAndrew and Sara S. Koehnke. 2016. On the nature of creepiness. *New Ideas in Psychology* 43 (2016), 10–15.

[61] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376167

[62] Eleanor McLellan, Kathleen M. MacQueen, and Judith L. Neidig. 2003. Beyond the qualitative interview: Data preparation and transcription. *Field Methods* 15, 1 (2003), 63–84. https://doi.org/10.1177/1525822X02239573

[63] Sascha Meinert. 2014. *Field Manual: Scenario Building.* Technical Report. European Trade Union Institute, Berlin. 1–27 pages.

[64] Marina Micheli, Marisa Ponti, Max Craglia, and Anna Berti Suman. 2020. Emerging models of data governance in the age of datafication. *Big Data & Society* 7, 2 (2020). https://doi.org/10.1177/2053951720948087

[65] Adam Moore. 2007. Privacy Rights. Moral and Legal Foundations, Pennsylvania.

[66] Deirdre K. Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083 (2016), 20160118. https://doi.org/10.1098/rsta.2016.0118

[67] Guillaume Nadon, Marcus Feilberg, Mathias Johansen, and Irina Shklovski. 2018. In the user we trust: Unrealistic expectations of Facebook's privacy mechanisms. In *Proceedings of the 9th International Conference on Social Media and Society* (Copenhagen, Denmark) *(SMSociety '18)*. Association for Computing Machinery, New York, NY, USA, 138–149. https://doi.org/10.1145/3217804.3217906

[68] Jennifer Nedelsky. 1990. Law, boundaries, and the bounded self. *Representations* 30 (1990), 162–189.

[69] Christena E. Nippert-Eng. 2010. *Islands of privacy.* University of Chicago Press, Chicago, IL.

[70] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79 (2004), 119–158.

[71] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press, Stanford, CA.

[72] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[73] President's Council of Advisors on Science and Technology (US). 2014. *Report to the President, Big data and privacy: A technology perspective.* Executive Office of the President, Washington, D.C.

[74] Ihudiya Finda Ogbonnaya-Ogburu, Angela D. R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical race theory for HCI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3313831.3376392

[75] Paul Ohm. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.* 57 (2009), 1701.

[76] Susanna Paasonen. 2015. As networks fail: Affect, technology, and the notion of the user. *Television & New Media* 16, 8 (2015), 701–716.

[77] Emmi Parviainen and Marie Louise Juul Søndergaard. 2020. Experiential qualities of whispering with voice assistants. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376187

[78] Scott R. Peppet. 2011. Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Nw. UL Rev.* 105 (2011), 1153.

[79] Sandra Petronio. 2002. *Boundaries of privacy: Dialectics of disclosure.* SUNY Press, Albany, NY.

[80] James Pierce. 2019. Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300275

[81] Emilee Rader. 2014. Awareness of behavioral tracking and information privacy concern in Facebook and Google. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 51–67. https://www.usenix.org/conference/soups2014/proceedings/presentation/rader

[82] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. 2020. "I have a narrow thought process:" Constraints on explanations connecting inferences and self-perceptions. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Virtual, 457–488. https://www.usenix.org/conference/soups2020/presentation/rader

[83] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 6, 17 pages. https://doi.org/10.1145/2335356.2335364

[84] Julian Rappaport. 1985. The power of empowerment language. *Social Policy* 16, 2 (1985), 15–21.

[85] Hanna Schneider, Malin Eiband, Daniel Ullrich, and Andreas Butz. 2018. Empowerment in HCI - A survey and framework. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173818

[86] Natasha Dow Schüll. 2016. Data for life: Wearable technology and the design of self-care. *BioSocieties* 11, 3 (2016), 317–333.

[87] John S. Seberger and Geoffrey C. Bowker. 2020. Humanistic infrastructure studies: Hyper-functionality and the experience of the absurd. *Information, Communication & Society* 0, 0 (2020), 1–16. https://doi.org/10.1080/1369118X.2020.1726985

[88] Martin E. P. Seligman. 1972. Learned helplessness. *Annual review of medicine* 23, 1 (1972), 407–412.

[89] Frank M. Shipman and Catherine C. Marshall. 2020. Ownership, privacy, and control in the Wake of Cambridge Analytica: The relationship between attitudes and awareness. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376662

[90] Irina Shklovski, Louise Barkhuus, Nis Bornoe, and Joseph 'Jofish' Kaye. 2015. Friendship maintenance in the digital age: Applying a relational lens to online social interaction. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1477–1487. https://doi.org/10.1145/2675133.2675294

[91] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421

[92] Herbert A. Simon. 1990. Bounded Rationality. In *Utility and Probability*, John Eatwell, Murray Milgate, and Peter Newman (Eds.). Palgrave Macmillan UK, London, 15–18. https://doi.org/10.1007/978-1-349-20568-4_5

[93] Judith Simon. 2015. Distributed epistemic responsibility in a hyperconnected era. In *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Luciano Floridi (Ed.). Springer International Publishing, Cham, 145–159. https://doi.org/10.1007/978-3-319-04093-6_17

[94] Daniel J. Solove. 2005. A taxonomy of privacy. *U. Pa. L. Rev.* 154 (2005), 477.

[95] Daniel J. Solove. 2008. Understanding privacy. May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420, Available at SSRN: https://ssrn.com/abstract=1127888.

[96] Daniel J. Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.

[97] Felix Stalder. 2002. The failure of privacy enhancing technologies (PETs) and the voiding of privacy. *Sociological Research Online* 7, 2 (2002), 25–39.

[98] Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security Fatigue. *IT Professional* 18, 5 (2016), 26–32. https://doi.org/10.1109/MITP.2016.84

[99] Luke Stark. 2016. The emotional context of information privacy. *The Information Society* 32, 1 (2016), 14–27.

[100] Cass R. Sunstein. 2015. Nudging and choice architecture: Ethical considerations. (January 17, 2015). Yale Journal on Regulation, Available at SSRN: https://ssrn.com/abstract=2551264.

[101] Herman T. Tavani. 2008. Informational privacy: Concepts, theories, and controversies. In *The handbook of information and computer ethics*, Kenneth E. Himma & Herman A. Tavani (Ed.). John Wiley & Sons, Hoboken, NJ, 131–164.

[102] Omer Tene and Jules Polonetsky. 2013. A theory of creepy: Technology, privacy and shifting social norms. *Yale JL & Tech.* 16 (2013), 59.

[103] Richard H. Thaler and Cass R. Sunstein. 2009. *Nudge: Improving decisions about health, wealth, and happiness.* Penguin, New York.

[104] Zeynep Tufekci. 2018. Facebook's surveillance machine. New York Times, March 19, 2018.

[105] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 4, 15 pages. https://doi.org/10.1145/2335356.2335362

[106] Janet Vertesi, Jofish Kaye, Samantha N. Jarosewski, Vera D. Khovanskaya, and Jenna Song. 2016. Data narratives: Uncovering tensions in personal data management. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 478–490. https://doi.org/10.1145/2818048.2820017

[107] Robin Wakefield. 2013. The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems* 22, 2 (2013), 157–174.

[108] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 309–325. https://www.usenix.org/conference/soups2015/proceedings/presentation/wash

[109] Alan F. Westin. 2015. *Privacy and Freedom.* IGI Global, Hershey, PA.

[110] Dylan Eric Wittkower. 2016. Lurkers, creepers, and virtuous interactivity: From property rights to consent and care as a conceptual basis for privacy concerns and information ethics. *First Monday* 21, 10 (Sep. 2016). https://doi.org/10.5210/fm.v21i10.6948

[111] Verena M. Wottrich, Eva A. van Reijmersdal, and Edith G. Smit. 2018. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems* 106 (2018), 44–52.

[112] Justin Wu, Cyrus Gatrell, Devon Howard, Jake Tyler, Elham Vaziripour, Kent Seamons, and Daniel Zappala. 2019. Something isn't secure, but I'm not sure how that translates into a problem: Promoting autonomy by designing for understanding in Signal. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '19)*. USENIX Association, USA, 137–153.

[113] Jason C. Yip, Kiley Sobel, Xin Gao, Allison Marie Hishikawa, Alexis Lim, Laura Meng, Romaine Flor Ofiana, Justin Park, and Alexis Hiniker. 2019. Laughing is scary, but farting is cute: A conceptual model of children's perspectives of creepy technologies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland UK) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300303

[114] Bo Zhang and Heng Xu. 2016. Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1676–1690. https://doi.org/10.1145/2818048.2820073

[115] Hui Zhang, Munmun De Choudhury, and Jonathan Grudin. 2014. Creepy but inevitable? The evolution of social networking. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 368–378. https://doi.org/10.1145/2531602.2531685

[116] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376570

[117] Shoshanna Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs, New York.

A SCREENING QUESTIONNAIRE

Thank you for your interest in participating in our study on People's Perceptions of Technology-Related Scenarios.

Please fill out this brief questionnaire about yourself. We will use your answers to determine if you are eligible to participate in the study.

If you qualify, we will contact you via email for a 45- to 60-minute interview. As a token of our appreciation for your participation in the interview, you will receive $10 cash or cash equivalent, such as an Amazon gift certificate. If you do not qualify for participation, your responses will be safely discarded.

- What is your year of birth?
- What is your gender?
- How long have you lived in the United States?
- Are you a resident of Bloomington, Indiana?
- Are you affiliated with Indiana University Bloomington?
- (If yes to previous question) What is your affiliation with Indiana University?
- (If student) What is your major/field of study?
- (If student) What department or school are you affiliated with?
- If you qualify for the study, which email address should we use to contact you for scheduling an interview?

B INTERVIEW PROTOCOL

Thanks for taking the time to talk with me today. As you read in the Study Information Sheet, we are trying to understand how people feel about technology in their daily lives. In order to get a sense of your feelings and opinions, I am going to have you read and think about a series of technology-related scenarios. After you read each scenario, we will have a discussion before proceeding to the next scenario.

Before we get to the scenarios, could you tell me a bit about yourself:

- What do you do and what are your interests?
- How do you use technology in your daily life?
- How do you typically select the technologies you use?
- How do you deal with any technology-related challenges?

Now let's discuss some scenarios related to technology.

Scenario 1:
You have installed an app that can identify music tracks by listening to them. From this, the app creates a 'weekly top chart' of songs you listen to the most. The data about your listening habits is used to tailor music ads within the app. You can't remove the ads.

- How often would you use such an app?
- What do you think about the app?
- What do you think about the track identification feature?
- What do you think about the "weekly top chart" feature?
- What do you think about the tailored ads?
- How do you think the app would operate?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 2:
You have installed an app to help you keep track of what you eat by inputting the food you eat throughout the day. The next day, a friend informs you that the people making the app are selling the collected information to local grocery store chains. You can select which grocery store chains will receive your data.

- How often would you use such an app?
- What do you think about the app?
- What do you think of a tool that helps keep track of the food you eat?
- How do you feel about the app makers selling the collected information?
- Does it matter that you can pick the grocery store chains to which the data can be sold?
- Does it matter that the stores are local?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 3:
You have installed a messenger app that can do voice recordings that you can send instead of text messages. The app has access to your microphone, and it will periodically record sound if it recognizes someone speaking. The recordings you make as well as the random sampling of ambient sound are sent to the company that makes the app to improve their services and to third party advertisers. By paying for the app, you can prevent the app from recording ambient sound and from sending any data to third parties. The app will still continue to send data to the company for service improvement purposes.

- How often would you use such an app?
- What do you think about the app?
- What do you think of voice-to-text features?
- How do you feel about the app recording sound when it recognizes someone speaking?
- What about when it randomly records ambient sound?
- How do you feel about those recordings being used to improve the app?
- How do you feel about those recordings being sold to third-party advertisers?
- How do you feel about paying for the app to prevent it from recording ambient sound or sending recordings to third parties?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 4:
You use an app to help you exercise better. One of the app features is a scoreboard that compares your performance with other app users. You can check out user profiles and see their individual scores, heart rate, and/or weight over time. You have the option of making your own profile private but doing so will prevent you from being added to the scoreboard.

- How often would you use such an app?
- What do you think about the app?
- What do you think about the scoreboard feature?
- What do you think about people looking at your statistics?
- What do you think about looking at other people's statistics?
- What do you think about the option to go private?
- Why would or wouldn't you want to share this information?
- What other types of information would you want to share?

- What configuration would work for you?
- Would you be interested in other people's statistics? Why or why not?
- Whose statistics would you want to see?
- What do you think about the people who make the app?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 5:
You book a flight using your Google Mail as the contact email address. As you open your calendar to enter the flight information, you notice that it has already been added automatically. You find a feature in Google Mail that enables or disables this service.

- How often would you use such a service?
- What do you think about this service?
- What do you think about your calendar updating automatically?
- How do you think the service knew to update the calendar?
- What do you think about the ability to enable or disable this service?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 6:
You voted for a different political party for the first time in many years. You start to notice that the party for which you voted suddenly seems to have a far stronger presence on social media. Your friends claim that they barely see anything from that party online.

- What do you think about this scenario?
- What do you think about the increased social media presence of the new party?
- Why do you think you are seeing an increase? (If appropriate) How does your reason/answer make you feel?
- What do you think about your friends seeing different things online compared to what you see?
- Why do you think they see different things?
- How do you think they found out how you voted? Does it matter?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 7:
You uploaded a photo from a family dinner to your Facebook account. A month later, you come across an ad that uses your photo. You have no way of challenging the use of the photo in the ad.

- What do you think about this scenario?
- If this were to happen, would you keep using Facebook?
- How might this change how you use Facebook?
- How often do use social media like Facebook?
- Do you upload photos to social media? Why or why not? If yes, how often?
- How do you feel about your photo being used in an ad?
- What do you think about being unable to challenge the photo in the ad?
- If you knew that this could happen, would you still use social media like Facebook? Why or why not?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.

Scenario 8:
You have been arguing a bit more than usual with your significant other over Facebook messenger. Over time, you start noticing ads for couple counseling and dating. You can tell Facebook that these ads are inappropriate.

- What do you think about this scenario?
- Do you use messaging services such as Facebook Messenger? Why or why not?
- How do you feel about seeing ads for couples counseling and dating?
- Why do you think you are seeing those ads?
- What do you think about the option to tell Facebook that these ads are inappropriate?
- If the participant expresses negative (or positive) opinions regarding ads or advertising, ask why.