Still Creepy After All These Years: The Normalization of Affective Discomfort in App Use

John S. Seberger
College of Communication Arts and Sciences
Michigan State University
East Lansing, Michigan, USA
seberge1@msu.edu

Irina Shklovski
Department of Computer Science and
Department of Communication
University of Copenhagen
Copenhagen, Denmark
ias@di.ku.dk

Emily Swiatek
Luddy School of Informatics, Computing, and Engineering
Indiana University Bloomington
Bloomington, Indiana, USA
eswiatek@iu.edu

Sameer Patil
School of Computing
University of Utah
Salt Lake City, Utah, USA
sameer.patil@utah.edu

ABSTRACT

It is not well understood why people continue to use privacy-invasive apps they consider creepy. We conducted a scenario-based study ($n = 751$) to investigate how the intention to use an app is influenced by affective perceptions and privacy concerns. We show that creepiness is one facet of *affective discomfort*, which is becoming normalized in app use. We found that affective discomfort can be negatively associated with the intention to use a privacy-invasive app. However, the influence is mitigated by other factors, including data literacy, views regarding app data practices, and ambiguity of the privacy threat. Our findings motivate a focus on affective discomfort when designing user experiences related to privacy-invasive data practices. Treating affective discomfort as a fundamental aspect of user experience requires scaling beyond the point where the thumb meets the screen and accounting for entrenched data practices and the sociotechnical landscape within which the practices are embedded.

CCS CONCEPTS

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

KEYWORDS

affective discomfort, affect, creepy, creepiness, data practices, privacy, privacy paradox, mobile apps

ACM Reference Format:
John S. Seberger, Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. Still Creepy After All These Years: The Normalization of Affective Discomfort in App Use. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3491102.3502112

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3502112

1 INTRODUCTION

People routinely claim that they find the data practices of many apps to be creepy [61, 73]. Yet, they do not necessarily refrain from using these apps [58]. Do actions speak louder than words or words louder than actions? Which of the two should be foregrounded when designing privacy solutions? After all, 'saying' and 'doing' are different things, and the difference is central to what is called the privacy paradox. The privacy paradox refers to a phenomenon wherein people *say* they value privacy but *act* in ways that seem to show little concern for it [1, 13, 34]. This "attitude-behavior gap" [81] continues to complicate research- and design-based attempts to help people manage privacy in the digital world. Several explanations have been proposed for why the privacy paradox persists. Some have even argued that the observed discrepancy is perhaps not paradoxical at all (e.g., [58, 63]). While people may want to protect their privacy in principle, it is possible that they do not see a realistic way to do so in practice. It is further possible that people have resigned themselves to having their privacy routinely violated [20, 58, 61], thus negating any meaningful differentiation between what they say and what they do.

Given that privacy is typically approached as a problem of data control [78], the user experience of privacy is implicitly rooted in experiences of violations – the moments when people realize that something is wrong or when the veil of personal control over data privacy is lifted [29]. Approaching privacy as a form of control places privacy solutions in the domain of calculus and rationality. Yet, experiences of violations are deeply *affective*.

Recently, researchers have taken affective aspects of privacy into account [58, 67] and gone beyond assessments of purely rational decision-making to understand how and why people make decisions about online data disclosure. Focusing on the emotional context of privacy tends to bring up negative affective experiences described by terms such as 'creepy,' 'scary,' or 'disconcerting' [73]. Creepiness in particular has inspired empirical investigations including the development of systematic approaches to quantify it [35, 82]. Recent focus on the experience of creepiness in quantitative terms

narrows the meaning of the concept to its particular features or to a range of emotional or aesthetic responses. At the same time, other empirical investigations seem to use creepiness as an umbrella term for a variety of feelings of discomfort that arise when people use privacy-invasive technologies or are faced with data-disclosure situations [48, 50, 61, 69, 73].

Research suggests that feelings of affective discomfort may be mitigated by giving users control over data practices of technology (see the extensive literature review by Acquisti et al. [2]). Yet, providing increased control over data disclosure may have counter-intuitive results [14]. A focus on control-oriented privacy design has led to a proliferation of privacy settings across apps and services. Complementary research efforts in the area of privacy literacy aim to raise awareness that would enable users to take advantage of the available settings and make well-informed decisions about data disclosures [37, 53]. However, such control may be illusory and claims of empowerment overstated [58]. Further, privacy literacy relies on a central conception of the user as a rational actor: *actual* privacy literacy is measured, even though people's *self-perceived* privacy literacy is likely what motivates action.

Despite advances in identifying factors relevant to privacy decisions, why people continue to use privacy-invasive apps and services that make them feel uncomfortable remains an unanswered question. We investigate this matter by considering different sources of affective discomfort and their relationship to perceived control over data disclosure and self-assessed data literacy. Specifically, we address the following research questions:

- **RQ1**: Does perceived privacy control matter for the intention to continue using apps that cause affective discomfort?
- **RQ2**: What role do perceived data literacy and affective discomfort play in the intention to continue using an app perceived to be invasive?

To answer these questions, we conducted a scenario-based online study ($n = 751$) in which participants answered a set of questions regarding imagined experiences with a fictional but familiar app. We varied the type of privacy violation and the availability of privacy control to understand how the intention to continue using the app is influenced by perceived privacy control, perceived data literacy, and affective discomfort.

We found that people's intentions to continue using a privacy-invasive app can be positively associated with the presence of privacy control and negatively associated with affective discomfort. However, when considered in conjunction with other relevant factors, including data literacy and views regarding data practices of the app, the influence of privacy control is nullified. The intention to use such apps is lower for those who have higher expectations for transparency and control regarding personal information. However, the influence of desire for greater operational transparency regarding potentially privacy-invasive data practices seems to be softened when these practices are perceived to align with how people expect typical real-world apps to operate. Moreover, when ambiguously-specified data practices are considered to align with such expectations, affective discomfort is apparently not enough to deter people from using apps that employ such practices.

Based on these findings, we make the following contributions:

- show that the assumed importance of providing users with privacy control is mitigated by perceived data literacy and affective discomfort;
- reveal that the influence of affective discomfort depends on the nature of invasiveness of data practices;
- demonstrate that affective discomfort has become a normalized aspect of app use; and
- broaden the scope and scale of the consideration of privacy-related user experiences and corresponding sociotechnical solutions.

In the following sections, we situate our approach to the study of affective discomfort in the relevant literature. We use the literature to derive and justify four hypotheses. We then provide a detailed description of our study design and deployment. Subsequently, we present statistical analyses to test the hypotheses and answer the research questions posed above. We proceed to discuss the findings in-depth and place them within the broader landscape of privacy studies in Human-Computer Interaction (HCI). Next, we present several implications for human-centered privacy research and conclude with remarks on the importance of considering affective discomfort for understanding privacy-related user experiences.

2 RELATED WORK

Privacy is multi-faceted. Since privacy appears as a site of breakdown or controversy in a great many personal, social, and institutional contexts, it is difficult to pin down the discourse itself, let alone to identify solutions. Consequently, there are several different threads that deal with privacy within HCI, including relational privacy [7, 9, 18, 41], contextual integrity [12, 44], and power-oriented privacy [39, 58]. Social scientific approaches, such as those grounded in economic rationale (e.g., [4]) and psychological constructs (e.g., [2, 61, 67]), are also common.

From an economic-historical perspective, Acquisti et al. [4] demonstrated that privacy is a moving target.[1] Privacy problems become visible when the technologies of daily life break down [29] or function in unexpected ways [57]. New technologies are constantly emerging, often carrying with them new problems [75] and challenging existing social norms [72]. When technology challenges social norms, it can feel creepy and elicit feelings of discomfort [72]. That is, there is something deeply *affective* about privacy [67], precisely because privacy is frequently encountered through failure [29] and promises of control that are inherently, if unintentionally, suited to be broken [47].

Despite critiques of privacy as a broken promise [47] and the intriguing proposition that privacy exists only in its negative state [29], privacy research has successfully yielded various suggestions to help users mange their privacy. For instance, privacy researchers have proposed an array of ad hoc potential solutions to privacy problems. Such solutions include Privacy Enhancing Technologies (PETs) (e.g., [5]), Privacy by Design (PbD) practices (e.g., [68]), and privacy notices (e.g., [3, 19, 21]).

Through such solutions, the relevance of privacy is continually reasserted and refined alongside the evolving digital ecology in

[1] We note, however, that the history of privacy as a concept is much longer than is routinely acknowledged within HCI (cf. [28, 74]).

which it is situated [29]. Yet, an insistence on control-based conceptions of privacy (e.g., [78]) has led to a relative lack of attention to people's emotional responses to privacy violations and their role in decision-making and behavior. As Nussbaum wrote, "Emotions are not just the fuel that powers the psychological mechanism of a reasoning creature, they are parts, highly complex and messy parts, of this creature's reasoning itself" [46, p. 3]. Building on recent efforts [58, 67], we adopt an affective approach to privacy as a way to reconsider the fundamental issue of the privacy paradox. Below, we first review the salient literature on the privacy paradox. We then turn to the literature on privacy control and affect to situate and justify several hypotheses about factors associated with the intention to use privacy-invasive and apparently 'creepy' apps.

2.1 The Privacy Paradox

When it comes to digital privacy, people tend to say one thing and do another. Such a discrepancy between what is said and what is done constitutes the core of the contemporary discourse of the privacy paradox [1, 13, 34]. People – users and developers alike – want to achieve this nebulous state called 'privacy,' but don't readily know how to do so. Uncertainty about how to achieve privacy is all the more frustrating because privacy issues in technology are often highlighted in the popular media [60] and are consistently described as important to people [2] and policymakers [1, 36].

While the privacy paradox has been a cornerstone of privacy research for decades [16], it has recently come under increased scrutiny [58, 63]. In 2017, Barth and de Jong [13] identified no fewer than thirteen ways of understanding or rationalizing the privacy paradox. The most common approaches involve privacy calculus (e.g., [83]) based on people's rational assessments of benefits and trade-offs relative to disclosing private information [13]. Essentially, these approaches locate the privacy paradox in the role that rational risk assessment plays in privacy-related behavior.

Recently, Solove [63] has gone so far as to call the privacy paradox a myth, highlighting a catastrophic (methodo)logical problem. Others [2] have noted that the privacy paradox does not adhere to the logical requirements of Quine's [51] 'vertical paradox,' but is inappropriately held to related standards. Solove [63] argues that the 'paradox' results from extrapolating findings across two incommensurable scales: specific and well-defined situations and general attitudes. On the one hand, people's privacy-related actions are routinely measured in particular situations. When measured in such a manner, privacy-related behavior is highly specific and grounded in non-generalizable contexts. On the other hand, Solove [63] argues that people's expectations of privacy are too general and nebulous to account for every specific situation. In essence, actions in specific contexts do not scale to general concerns, especially since the set of possible contexts keeps expanding through new technologies and data practices.

Relatedly, Seberger et al. [58] showed that affect and conditional empowerment influence the relationship between privacy attitudes and behavior. In the context of app use, people routinely feel deceptively empowered [58], fatalistic toward the inevitability of privacy violations [20, 61], and overwhelmed by the responsibility for managing their privacy [1, 27, 62]. In this light, affect casts as large a shadow over the discourse of privacy as the privacy paradox.

2.2 Privacy Control and Data Literacy

Control over information is central to modern definitions of privacy [78]. As a consequence, if people say they value privacy, then designers tend to enable them to control their privacy. However, more control does not necessarily mean more privacy [14]. End-user privacy control may instead overburden users [62]. Further, the provision of such privacy control may contribute to the phenomenon of conditional empowerment [58] and associated negative affective outcomes, such as learned helplessness [61], resignation [20], and fatigue [23, 65]. A downward spiral of violated expectations [82], broken promises [47], and resignation [20, 61] ensues.

The effects of conditionally empowering [58] people with control over their data privacy are uncertain. Yet, people show a tendency to engage in risky privacy-related behavior when they perceive such control to be present [14]. If the presence of privacy control leads to an increase in risky privacy-related behavior and engaging in such risk requires use, then the perception of increased privacy control may increase use even when the technology is judged to be privacy-invasive. Therefore, we formulated the following hypothesis:

> **H1**: The perceived presence of privacy control is associated with increased intention to continue using a privacy-invasive app.

Yet, the provision of end-user privacy control and its relationship to the perception of agency is likely mediated by other factors as well. For instance, some research efforts point to the importance of privacy literacy for influencing privacy-related behavior [54]. Even though control-oriented privacy approaches implicitly emphasize rational considerations of risk [26] instead of affect, privacy literacy can still be important for understanding and exercising privacy control [54].

We consider privacy literacy as subsumed by a broader notion of *data* literacy [55]: people's critical understanding of the data practices of the technologies they use. Prior work has identified the role that data literacy plays in non-use of privacy-invasive technologies [45]. Yet, as with the difference between saying and doing, there is a real difference between *actual* data literacy and *perceived* data literacy. If people perceive themselves to possess high levels of data literacy, whether true or not, it is only logical that they might overestimate their ability to manage their privacy when using an invasive app. Therefore, when forming the following hypothesis, we used 'perceived data literacy' to refer to how people judge themselves to understand the data practices of apps and technologies:

> **H2**: Perceived data literacy is positively associated with the intention to continue using a privacy-invasive app.

2.3 Affect

Interventions founded in privacy calculus (cf. [13]) typically fail to account for the gap between 'saying' and 'doing.' When the privacy paradox is approached as a rationalistic problem of misalignment between valuation (i.e., saying) and behavior (i.e., doing) [63], it implicitly excludes its own possible explanation: the importance of affective perceptions and experiences that contextualize human rationality [46], including privacy decisions. We contend that the privacy paradox is not paradoxical when seen from an affective

point of view [32, 43, 67]. Therefore, we turn to a discussion of how privacy-related affective discomfort is understood in HCI.

Affective approaches to privacy (e.g., [67]) are becoming more common in HCI. Notably, much affective privacy work focuses on negative experiences, such as creepiness [48, 58, 61, 69, 85]. The first HCI work on the phenomenon of creepy user experiences is now ten years old [73]. Following the publication of this work, a subset of computing researchers interested in creepiness began to coalesce [61], with the subsequent expansion of creepiness research into the fields of psychology and legal studies (e.g., [15, 30, 35, 38, 77]). In recent years, several major studies about creepiness have been published by the HCI community (e.g., [58, 82, 84]).

Wozniak et al. [82] divide creepiness research in HCI into three areas: (i) (usable) privacy (e.g., [49, 61, 73]); (ii) Human-Robot Interaction (HRI) (e.g., [31, 56, 84]); and (iii) social acceptability (e.g., [33, 82]). Each of these areas is strongly oriented toward actionable implications for design. The study of creepiness in usable privacy, for example, aims to improve transparency and end-user privacy control, thereby ostensibly reducing the likelihood of experiencing creepiness (see Wozniak et al. [82] for a summary of this thread); creepiness research in HRI focuses on making the visual appearances of robots less creepy to users [64, 84]; and social acceptability concerns itself with the contextual nature of creepiness or with fitting new technologies into existing social norms (cf. [72]).

Creepy user experiences in technology use can arise from first impressions and aesthetics [82], violation of expectations [61], and perceived social unacceptability [73]. Within social informatics, creepy user experiences have been discussed through the existentialist lens of absurdity [57]. A closer look at the language of HCI literature on creepiness reveals that creepiness signifies a broader category of affective experiences. We refer to this category as 'affective discomfort.' Indeed, creepiness has been defined as emotional discomfort [42], with various negative emotional outcomes: repulsion, disturbance, apprehension, fright, or shock [49, 61, 73, 76, 80]. We would expect people to avoid using an app that evokes such feelings, leading us to the following hypothesis:

> **H3**: Affective discomfort is negatively associated with the intention to continue using a privacy-invasive app.

Creepy user experiences are a part of an emergent app culture characterized by the economics of surveillance capitalism and widespread digital resignation [20]. Seberger et al. [58] argue that apps only conditionally empower their users, giving them the 'power to' do certain things. However, that 'power to' exists within the context of the 'power over' constituted in the apps and their institutional backends. The disparity in 'power to' and 'power over' – what Seberger et al. [58] refer to as the difference between capability and capacity – likely contributes to privacy-related learned helplessness [61] that forms a condition of use conducive to ambivalence. Therefore, we would expect ambivalence toward invasive data practices of an app to increase the intention to use it. When ambivalent toward invasive data practices, a person's default inclination would be to use the app as captured by the following hypothesis:

> **H4**: Ambivalence toward the data practices of a privacy-invasive app is positively associated with the intention to continue using the app.

3 METHOD

In order to address our research questions and hypotheses, we designed a scenario-based, between-subjects study. We presented each participant with one of several versions of a core scenario describing the use of a mobile app. We followed Meinert's [40] guidelines for scenario development by creating a core scenario and systematic variations of it that were realistic and open to interpretation, without priming 'right or wrong' answers [58]. The core scenario described data practices of a music-identification app based on a similar scenario in the literature [58]. We systematically varied the core description to create different variations meant to elicit different types of affective discomfort. Prior work on creepiness and privacy has highlighted several underlying factors that make people uncomfortable in their experiences with technologies [61, 85]. These factors include: (i) violation of expectations, (ii) violation of personal boundaries, and (iii) ambiguity of threat [58, 82]. We designed three variations of the core scenario, each connected to one of the above three underlying factors. We generated two versions of each of the three variations, one with and one without user control over privacy aspects. The three variations with two versions each and the control version constitute the seven conditions in the study.

To ensure clarity of each scenario version, we conducted pilots with colleagues and acquaintances diverse in age, gender, ethnicity, education, and native language. Based on feedback from the pilots, we made several edits, including a reduction in length and simplification of grammatical structure, and used the refined versions in the study. The study procedures were reviewed and approved by the Indiana University Institutional Review Board (IRB).

3.1 Scenarios

Below we detail the core scenario used as the control and its systematic variations used in the treatment conditions. The full text of each scenario version is available in Appendix A.

3.1.1 Core Scenario. The core scenario describes a fictional music-identification app called Remember Music. It situates the app within a specific use case and provides detail about its data practices:

> Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.

The core scenario was written to describe a realistic experience users might have after downloading a free music-identification app. We included personalized advertising as a given despite it being previously described as creepy [73, 85]. By including personalized advertising within the core scenario, we aimed to facilitate the detection of meaningful differences between a hyper-realistic normalized control condition and variations thereof. While the

conservative approach would have been to exclude personalized advertising from the core scenario because it is potentially creepy, we felt that it would have been less realistic given current practices [58], thus violating Meinert's [40] guidelines for scenarios. Therefore, the core scenario reflects the commonly-encountered 'real-world' creepiness of apps that employ personalized advertising.

We systematically varied the core scenario by augmenting it with additional information to generate a version corresponding to the six treatment conditions mentioned above.

3.1.2 Violation of Expectations (VE). The first variation communicates a relatively common violation of expectations regarding the types of data an app might collect. This is a familiar type of expectation violation where an individual might discover, for instance, that an app collects superfluous location information even though its function does not necessarily or obviously call for it. In this variation, we included a notification from the Remember Music app that implies that the app uses location data:

> Today, you received an email from Remember Music recommending songs that 'your neighbors and people near you are listening to now.' You were not aware that the app used location data.

We then added text related to the presence or absence of corresponding privacy control to generate the two respective versions for this variation. The version with the possibility for exercising control over privacy (VE/C) indicates that users can limit the collection of location data:

> You navigate to Remember Music's settings on your phone and find a tab called 'Location Data.' Preferences within this tab allow you to prevent the app from using your location data to share with others what you are listening to now. You prevent the app from using your location and receive a confirmation that your preferences have changed.

In contrast, the version without privacy control (VE/NC) suggests that users cannot change what data Remember Music collects:

> You can't find a way to change Remember Music's access to your location data.

3.1.3 Breach of Personal Boundaries (PB). The second variation covers situations in which the data practices of an app violate personal boundaries. In this variation, we described a potentially uncomfortable situation where Remember Music exposes user activities on social media without the user's knowledge:

> Today, when you opened your social media account, you saw that Remember Music has inserted a publicly visible sidebar on your profile that allows your social network to see your music listening history. In your case, it includes several graphic images associated with some of the songs in your listening history. You don't want your coworkers and family to see these images.

We generated the two versions of this variation with additional text about privacy control or lack thereof. The version that includes privacy control (PB/C) mentions the option to stop the app from disclosing information on social media:

> You navigate to Remember Music's settings on your phone and find that you can turn off social media data sharing. After selecting that option, you navigate back to your social media page, and the Remember Music sidebar is gone. You receive a confirmation that your preferences have changed.

The version without privacy control (PB/NC) suggests that users cannot change app behavior related to disclosing information on social media:

> [...] but you can't find a way to change Remember Music's social media sharing settings.

3.1.4 Ambiguity of Threat (AT). The third variation is connected to situations where an app might collect data by 'listening in' on ambient conversation and using the data for personalized advertising. Such situations are not unrealistic given the widespread adoption of voice-based virtual assistants, such as Alexa or Siri. This variation is most likely to elicit a feeling of ambiguity of threat, where an individual may imagine that data practices such as ambient listening are plausible, but have no evidence that they are in fact happening. Moreover, an app eavesdropping on intimate private conversations without having been invoked via a 'wake word' is a more invasive violation, where the app clearly gathers more data than anticipated:

> Remember Music informs you that 'an artist you have been interested in lately will be playing nearby.' You have been talking with your partner a lot about the artist, but you haven't used Remember Music to search for songs by the artist. You do not know how or why you received this recommendation.

Ambient listening is a notoriously creepy data practice [30, 72]. The creepiness of Remember Music's likely ambient listening is augmented by its apparent use of location data, as indicated by the phrase 'playing nearby.'

We added the following text to generate the version of this variation with privacy control (AT/C):

> You navigate to Remember Music's settings on your phone, where you find a description of the app's data-sharing practices. You do not recall opting in to receive this type of notification, but easily identify how to opt out. You receive a confirmation that you will no longer receive recommendations for concerts in your area.

For the version without privacy control (AT/NC), we did not include specific additional text, relying simply on:

> You do not know how or why you received this recommendation.

Privacy control manifests slightly differently in the AT variation than in the other two. In the AT/C version, users can control whether they will receive notifications about concerts in their area, but not the collection of data that would make such recommendations possible. Similarly, the AT/NC version provides no information at all about why the app acts this way, foregrounding ambiguity. To increase the openness to interpretation [40] of the variation as well as the ambiguity central to it, we indicated that the person does not recall choosing to use the described feature of the app.

Table 1: Items to measure Affective Perceptions by adapting original CRoSS items. The iterms are further customized to the context of the Remember Music app described in the scenario used in the study.

Original Items from CRoSS	Items Adapted to Measure Affective Perceptions
During this situation, things were going on that I did not understand.	I understand how Remember Music uses the data it collects.
During this situation, I did not know exactly what was happening to me.	I understand what kinds of data Remember Music collects.
I did not know exactly what to expect of this situation.	I expect complications when I start using Remember Music.
I felt uneasy during this situation.	I would be comfortable with the way Remember Music uses my data.
I had a feeling that there was something shady about this situation.	I have a feeling that there is something shady about Remember Music.
I felt uneasy about this situation.	I think the way that Remember Music uses my data is absurd.
I had an unidentifiable fear during this situation.	I think the Remember Music app is creepy.

The inclusion of this indication contributes to realism given that people routinely click through user agreements without reading them. For the same reasons, we were intentionally ambiguous regarding the types of data collected (i.e., the possibility that data might be gathered through ambient listening or other means, such as third-party data brokers).

3.2 Questionnaire Components

Those who consented to participate and committed to providing thoughtful answers [6] proceeded to the questionnaire that randomly presented one of the above versions of the scenario followed by questions on three sets of measures: (i) a custom set of questions designed to measure Affective Perceptions; (ii) the App Information Privacy Concerns (AIPC) scale [17]; and (iii) the General Digital Difficulties subscale of the Digital Difficulties scale [8] for gauging general technical expertise. Next, we asked for information on the smartphone operating system, frequency of changing privacy settings, and the number of apps installed. At the end of the questionnaire, we collected standard demographics. Additionally, the questionnaire included four attention checks designed to filter out faithless respondents [24, 59]. No questions were mandatory; participants could choose to skip any question they did not wish to answer. The full questionnaire is included in Appendix B.

3.2.1 Measures of Affective Perceptions. A handful of scales, such as the CReepiness of Situations Scale (CRoSS) [35] and the Perceived Creepiness of Technology Scale (PCTS) [82], have been developed to measure creepiness. However, the items included in existing scales are not adequately formulated to measure the variables central to our research questions and hypotheses. Therefore, we developed our own measures for capturing various affective perceptions connected to app use.

To that end, we adapted items from the Emotional Creepiness and Creepy Ambiguity subscales of CRoSS [35]. The Emotional Creepiness subscale measures the "rather unpleasant affective impression elicited by unpredictable people, situations, or technologies" [35], and the Creepy Ambiguity subscale measures "a lack of clarity on how to act and how to judge in such a situation" [35].

While CRoSS includes items designed to measure creepiness in different contexts – involving people, technologies, and situations – we tailored our adaptations to the fictional app, Remember Music, included in the scenario. Data practices of apps mediate people's interactions and influence their perceptions. Therefore, where possible and relevant, we took inspiration from CRoSS items and specified Remember Music and its data practices as the object of otherwise generic situations presented in the CRoSS items. Table 1 lists the original and adapted wording of these CRoSS items.

We constructed a few additional items to measure aspects of Affective Perceptions not included in existing scales:

Intention to Continue Use: "I would continue to use Remember Music based on the scenario."
Perceived Realism of Data Practices: "I think the manner in which Remember Music uses my data is realistic."
Ambivalence Toward Data Practices: "I do not know how to feel about how Remember Music uses my data."

The full set of CRoSS-inspired and custom Affective Perception items is included in Appendix B.4.

3.2.2 AIPC Scale. Given our focus on reactions to app data practices, we included the AIPC scale [17] consisting of three validated subscales: (i) Anxiety (general concern for how apps might use and process personal data); (ii) Personal Attitude (importance of careful handling of personal data); and (iii) Requirements (expectations for transparency regarding data practices and provisions for controlling them). We excluded one item from the Personal Attitudes subscale ("When mobile apps ask me for personal information, I sometimes think twice before providing it.") because we deemed it to be related to behavior rather than attitude.

3.3 Data Collection and Sample Characteristics

We used the questionnaire to conduct a between-subjects online study advertised as a Human Intelligence Task (HIT) on the Amazon Mechanical Turk (AMT) platform between April 21 and June 18, 2021. AMT has been shown to be a suitable means of studying relatively young (18-50) and well-educated Americans [52]. The

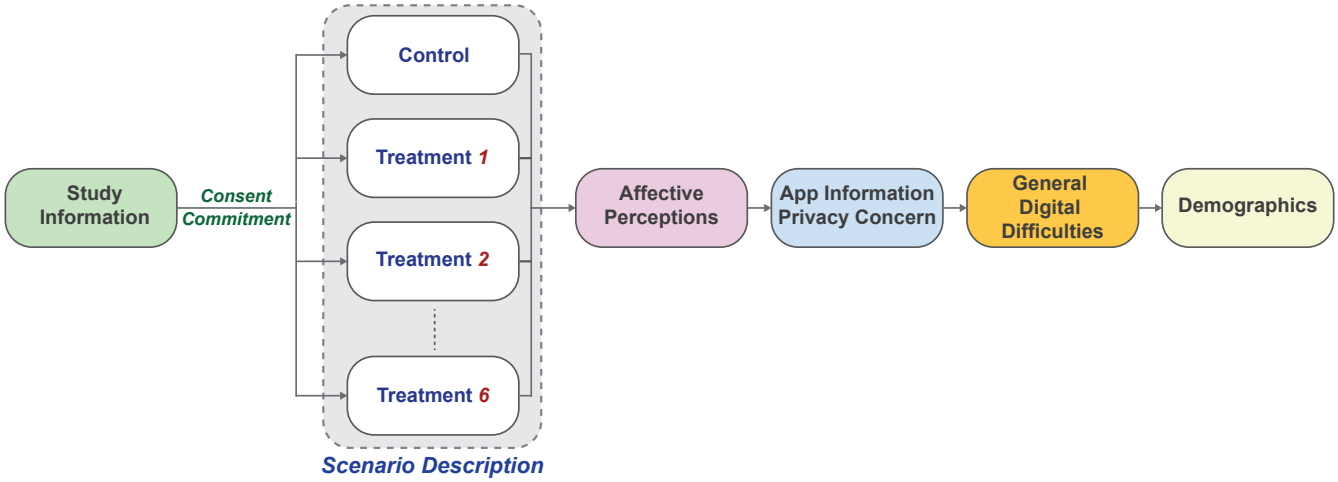

Figure 1: The overall flow of the components of the between-subjects study.

study consisted of one control and six treatment conditions, corresponding to the versions of the scenario presented above.

Figure 1 shows the overall flow of the study procedures. Those who accepted the HIT and visited the questionnaire link were first shown detailed information about the study procedures to seek informed consent for participation. Those who did not consent to participate or commit to providing thoughtful answers were asked to return the HIT on AMT. The rest were randomly assigned to one of the seven study conditions and proceeded to answer the questionnaire based on the version of the scenario corresponding to the study condition.

The median time to complete the study was about six minutes and thirty seconds. Upon completion of the study, participants were given a randomly-generated code to enter on AMT. Those who completed the study and entered the correct code on AMT received US $1.20, which translates roughly to a compensation of US $11 per hour which is more than 50% higher than the Federal minimum wage in the United States.

3.3.1 Eligibility and Exclusion Criteria. Residents of the United States 18 years of age or older were eligible to participate in the study. To ensure high response quality, we limited participation to those who had completed at least 50 HITs on AMT with a task approval rating of 95% or higher. To receive compensation, participants were required to provide correct answers to the four attention checks distributed across different parts of the questionnaire.

We received a total of 1,222 responses to our study. Of these, 465 were excluded for failing one or more attention checks. For statistical reasons, we removed responses of six participants who did not disclose gender (3), provided self-described gender (1), or identified as non-binary (2). Keeping the data from these six participants would not have affected the overall results given their very low proportion among the much larger sample. However, it would have prevented us from including gender in the statistical analyses because of a lack of sufficient statistical power due to the low number of participants in these gender categories (see Section 7). Applying these filters resulted in a sample of 751 complete and usable responses distributed roughly equally across the seven study conditions. Table 2 provides the distribution of participants across the six treatment conditions. In addition, we obtained 107 responses in the control condition.

3.3.2 Sample Characteristics. Of the 751 participants, 299 (40%) identified as women and 452 (60%) as men. Participant ages ranged from 18 to 78, with a median of 36. The sample contained a slightly higher proportion of those older than 35, with 416 (55%) participants aged 35 years or older and 335 (45%) between the ages of 18 and 34.

4 FINDINGS

We first examined the internal validity of the measures used in the study. Next, we confirmed the success of our treatments with an analysis of variance (ANOVA). Then, we investigated the isolated role of the presence of privacy control in the intention to continue using Remember Music with a one-way multiple analysis of variance (MANOVA) between the two versions of the scenario in each variation: VE/C and VE/NC; PB/C and PB/NC; AT/C and AT/NC.

Finally, we constructed multiple linear regression (MLR) models for each of the three variations to test our hypotheses (see Section 2) and understand how the intention to continue using the Remember Music app was influenced by privacy control, perceived data literacy, affective discomfort, the AIPC scale, age, and gender. For each of the three variations, we first analyzed the influence of privacy control independently. However, privacy control does not exist in a vacuum

Table 2: Distribution of responses across the six treatment conditions.

Privacy Control	Violation of Expectations **(VE)**	Breach of Personal Boundaries **(PB)**	Ambiguity of Threat **(AT)**
Yes **(C)**	115	105	102
No **(NC)**	115	104	103

Table 3: Principal Component Analysis (Varimax) for the ten items measuring Affective Perceptions showing five factors, which we labeled Affective Discomfort (Factor 1), Intention to Continue Use (Factor 2), Data Literacy (Factor 3), Ambivalence Toward Data Practices (Factor 4), and Perceived Realism of Data Practices (Factor 5). Items with a * were reverse-coded for analysis to ensure that the numeric responses for all items were consistent, with higher scores indicating higher negative affect.

	FACTORS					
Item	**1**	**2**	**3**	**4**	**5**	**Communality**
I have a feeling that there is something shady about Remember Music.	**0.86**	0.08	−0.01	−0.12	0.04	1.1
I think the Remember Music app is creepy.	**0.83**	0.17	−0.01	−0.03	0.17	1.2
I expect complications when I start using Remember Music.	**0.83**	−0.23	−0.05	0.11	0.08	1.2
I think the way Remember Music uses my data is absurd.	**0.81**	0.11	−0.07	0.04	0.20	1.2
I would be comfortable with the way Remember Music uses my data.*	0.00	**0.88**	0.28	0.11	−0.06	1.2
I would continue to use Remember Music based on the scenario.*	0.14	**0.82**	0.27	0.20	−0.07	1.4
I understand how Remember Music uses the data it collects.*	−0.06	0.35	**0.80**	0.14	0.04	1.5
I understand what kinds of data Remember Music collects.*	−0.05	0.19	**0.89**	0.13	0.01	1.1
I think the manner in which Remember Music uses my data is realistic.*	−0.01	0.26	0.23	**0.93**	0.01	1.3
I do not know how to feel about how Remember Music uses my data.	0.34	−0.12	0.05	0.00	**0.92**	1.3
Percent of Variance Explained	0.35	0.22	0.20	0.12	0.11	–
Cumulative Variance Explained	0.35	0.57	0.77	0.89	1.00	–

nor do beliefs about understanding of data practices (i.e., perceived data literacy). Therefore, we subsequently included privacy control as part of a broader exploration of associations between factors related to the intention to continue using the Remember Music app. In all cases, we initially checked for the influence of relevant interaction effects among the independent variables, but dropped these from the final models if they were not statistically significant.

4.1 Confirmatory Factor Analysis of the AIPC Scale

To check for internal consistency, we conducted a Confirmatory Factor Analysis (CFA) on the items contained within the AIPC scale. While the χ^2 (623.35, $df = 87$; $p < 0.001$) of the CFA is reasonable, the root mean square error of approximation ($RMSEA = 0.09$) indicates that the factors identified by the AIPC scale do not sufficiently explain the phenomenon of app privacy concerns when compared to an idealized or perfect model. On the other hand, the comparative fit index ($CFI = 0.91$) justifies the continued use of the AIPC subscales for the analyses in our study.

Although the CFA confirmed the loadings of individual items on the three subscales [17], we observed that the Anxiety subscale was highly correlated with the two other subscales (Anxiety – Personal Attitudes: $r = 0.86$ and Anxiety – Requirements: $r = 0.67$). We therefore made the decision to drop the Anxiety subscale of the AIPC scale in subsequent analyses.

4.2 Principal Component Analysis of Affective Perceptions

We verified that the ten items used to measure Affective Perceptions exhibited high internal consistency (Cronbach's $\alpha = 0.75$). In order to test the validity of the measures, we next performed a Principal Component Analysis (PCA) with varimax rotation to analyze the ten items taken together (see Table 3). As Table 3 indicates, for the purposes of the PCA, we reverse-coded five of the items such that the direction of numeric responses for all ten items was consistent, moving from lower to higher negative affect.

The results of the PCA yielded five factors with appropriate communality, suggesting that Affective Perceptions are composed of several underlying components. We labeled the first factor as 'Affective Discomfort,' because it is composed of items describing discomfiting aspects of app use: shadiness, creepiness, complications, and absurdity. The second factor, which we labeled 'Intention to Continue Use,' is associated with the two items related to the intention to continue app use. Items related to people's self-assessed understanding of app data practices load on Factor 3, which we labeled 'Perceived Data Literacy.' Based on the single items that load respectively on Factors 4 and 5, we labeled them as 'Ambivalence Toward Data Practices' and 'Perceived Realism of Data Practices,' respectively. We used these factors as variables when constructing the MLR models mentioned above. The items loading on each individual factor are similarly phrased in terms of the direction of negative affect. Therefore, we did not reverse code any items for the MLR models because the original numeric responses are more intuitive as the measure for each labeled factor. For example, the original numeric responses for the two items that measure the Perceived Data Literacy factor are ordered such that higher scores correspond to higher Perceived Data Literacy.

4.3 Differences Across Scenario Variations

In order to ensure that participants found the three variations (i.e., VE, PB, and AT) of the core scenario to be reasonably realistic, we conducted an ANOVA for differences in responses to the item, "I think the manner in which Remember Music uses my data is realistic," between the control condition and the three variations, with the responses for the two treatment versions (i.e., C and NC) for each variation combined. Results were not statistically significant

Table 4: Standardized β and standard error values for the predictor variables associated with the Intention to Continue Use of Remember Music as the outcome variable across all MLR models for the control and treatment conditions, with the treatments representing the respective versions with and without privacy control combined.

	Control		Violation of Expectations (VE)		Breach of Personal Boundaries (PB)		Ambiguity of Threat (AT)	
Predictor Variable	*Std*β	*StdErr*	*Std*β	*StdErr*	*Std*β	*StdErr*	*Std*β	*StdErr*
Privacy Control	—		0.00	0.10	−0.04	0.11	0.77	0.48
Perceived Data Literacy	**0.47**	**0.10*****	**0.49**	**0.05*****	**0.48**	**0.06*****	**0.48**	**0.06*****
Affective Discomfort	−0.03	0.11	**−0.20**	**0.06****	**−0.30**	**0.07*****	−0.07	0.07
Ambivalence Toward Data Practices	−0.08	0.10	**0.26**	**0.05*****	**0.29**	**0.06*****	0.00	0.07
Perceived Realism of Data Practices	**0.22**	**0.10***	**0.28**	**0.05*****	**0.19**	**0.06****	**0.24**	**0.08****
Personal Attitudes (AIPC subscale)	0.10	0.11	0.04	0.07	0.10	0.07	−0.03	0.07
Requirements (AIPC subscale)	0.11	0.10	**−0.19**	**0.06****	**−0.14**	**0.06***	**−0.22**	**0.06*****
Age (35+)	−0.13	0.15	−0.16	0.10	−0.04	0.10	−0.06	0.11
Gender (Female)	0.20	0.15	−0.03	0.10	0.14	0.11	0.12	0.11
Perceived Realism x Privacy Control	—		—		—		**−0.17**	**0.09***
Adjusted R^2	0.44		0.48		0.46		0.42	

Statistical significance levels: $^{*}: p < 0.05$ $^{**}: p < 0.01$ $^{***}: p < 0.001$

($F(3, 747) = 1.68, p = 0.17$), suggesting that participants perceived all variations of the core scenario to be realistic.

To confirm that the variations to the core scenario were successful in influencing participant perceptions of creepiness, we conducted an ANOVA that compared responses to the item, "I think the Remember Music app is creepy," between the control condition and the three variations. The results of the ANOVA ($F(3, 747) = 4.22$, $p = 0.006$) indicate that the treatments affected perceptions. Post hoc Tukey tests showed that perceptions of creepiness in treatments corresponding to all three variations were statistically significantly different from the control condition ($p = 0.004$, $p = 0.01$, and $p = 0.03$ for VE, PB, AT, respectively).

We further checked whether the variations to the core scenario influenced the intention to use Remember Music with an ANOVA that compared responses to the item, "I would continue to use Remember Music based on the scenario," between the control condition and the treatments corresponding to the three variations. We found that the treatments affected participant intentions to continue using Remember Music ($F(3, 747) = 4.87, p = 0.002$). Post hoc Tukey tests showed statistically significant differences between the control condition and VE ($p = 0.02$) as well as BP ($p = 0.005$) treatments. There was no statistically significant difference between the control condition and the AT treatments ($p = 0.53$).

4.4 Violation of Expectations (VE)

In the VE treatments, Remember Music was depicted as violating expectations by collecting superfluous types of data.

4.4.1 Privacy Control. We conducted a one-way MANOVA to test the effect of the presence of Privacy Control on four variables: Intention to Continue Use, Perceived Data Literacy, Affective Discomfort, and Ambivalence Toward Data Practices. The MANOVA yielded statistically significant results (Pillai's trace = 0.06, $F(1, 228) = 3.35$, $p = 0.01$). Follow-up ANOVAs showed that Intention to Continue Use was statistically significantly different between the VE treatments with and without privacy control ($F(1, 228) = 4.24, p = 0.04$). Further, the two VE treatments were statistically significantly different in the extent to which participants reported Affective Discomfort ($F(1, 228) = 3.77, p = 0.05$) and Perceived Data Literacy ($F(1, 228) = 6.27, p = 0.01$).

The above results indicate that the presence of privacy control, when considered by itself, is associated with a greater intention to continue using an app that violates expectations by collecting superfluous forms of data. In the absence of Privacy Control, participants were less likely to express the Intention to Continue Use of the app (NC mean = 4.34 and C mean = 4.77), experience greater Affective Discomfort (NC mean = 4.83 and C mean = 4.49), and report lower Perceived Data Literacy (NC mean = 4.71 and C mean = 5.18).

4.4.2 Intention to Continue Use. We used MLR for simultaneous examination of how the Intention to Continue Use of Remember Music when it violated expectations by collecting superfluous data is collectively influenced by the various factors mentioned above. The MLR model accounted for 48% of the variance in Intention to Continue Use (Adjusted $R^2 = 0.48$, $F(9, 220) = 24.08, p < 0.001$), with statistically significant influences of Perceived Data Literacy, Affective Discomfort, Ambivalence Toward Data Practices, Perceived Realism of Data Practices, and the Requirements subscale of the AIPC scale (see Table 4). Notably, we found no statistically significant relationship between Privacy Control and Intention to Continue Use, even though the treatment described the collection of superfluous types of data.

As expected, Affective Discomfort in the VE treatments was negatively associated with the Intention to Continue Use of Remember Music ($\beta = -0.20, p = 0.002$). Similarly, the Intention to Continue Use of Remember Music was negatively associated with the Requirements subscale of the AIPC scale ($\beta = -0.19, p = 0.001$). At the

same time, the Intention to Continue Use of the app was positively associated with Perceived Data Literacy ($\beta = 0.49$, $p < 0.001$), Ambivalence Toward Data Practices ($\beta = 0.26$, $p < 0.001$), and Perceived Realism of Data Practices ($\beta = 0.28$, $p < 0.001$).

Despite affective discomfort, those who expressed greater ambivalence about superfluous data collection and judged themselves to possess higher data literacy were more likely to continue app use the more they considered its data practices to be realistic, independent of privacy control. The intention to use was lower for those who placed higher importance on transparency and control for data handling (as captured by the Requirements subscale of the AIPC scale). However, the influence seems to be softened when potentially privacy-invasive practices were aligned with a general understanding of how apps typically operate (as captured by the Perceived Realism of Data Practices measure).

4.5 Breach of Personal Boundaries (PB)

In the PB treatments, Remember Music breached personal boundaries by unexpectedly sharing information with a user's social network, thus potentially risking negative social exposure.

4.5.1 Privacy Control. We conducted a one-way MANOVA to compare Intention to Continue Use, Perceived Data Literacy, Affective Discomfort, and Ambivalence Toward Data Practices between the PB versions with and without Privacy Control. The MANOVA was statistically significant (Pillai's trace = 0.1, $F(1, 207) = 5.46$, $p < 0.001$). Follow-up ANOVAs identified that Affective Discomfort differed statistically significantly based on the presence of Privacy Control ($F(1, 207) = 19.01$, $p < 0.001$). As in the VE treatments, the presence of Privacy Control was associated with lower Affective Discomfort (C mean = 4.19 and NC mean = 5.02). We observed no other statistically significant differences between the PB versions with and without privacy control.

4.5.2 Intention to Continue Use. The MLR model for examining how the Intention to Continue Use of Remember Music despite breach of personal boundaries is collectively influenced by the various factors mentioned above accounted for 46% of the variance (adjusted $R^2 = 0.46$, $F(9, 199) = 20.28$, $p < 0.001$). Similar to the VE treatments, there was no statistically significant relationship between Privacy Control and Intention to Continue Use despite the breach of personal boundaries included the PB treatments.

As seen in Table 4, the Intention to Continue Use of Remember Music in the PB treatments was negatively associated with Affective Discomfort ($\beta = -0.30$, $p < 0.001$) and the Requirements subscale of the AIPC scale ($\beta = -0.14$, $p < 0.03$). On the other hand, it was positively associated with Perceived Data Literacy ($\beta = 0.48$, $p < 0.001$), Ambivalence Toward Data Practices ($\beta = 0.29$, $p < 0.001$), and Perceived Realism of Data Practices ($\beta = 0.19$, $p = 0.003$).

As in the VE treatments, greater self-perceptions of data literacy and greater ambivalence about superfluous data collection were associated with a greater intention to continue using a boundary-violating app despite higher affective discomfort, regardless of the availability of privacy control. At the same time, as in the VE treatments, those who indicated higher intention to use such an app desired greater transparency and control for handling of personal data (as measured by the Requirements subscale of the AIPC scale), tempered by whether the potentially privacy-invasive practices were deemed realistic.

4.6 Ambiguity of Threat (AT)

In the AT treatments, the data practices of Remember Music were ambiguously threatening because the app was described as collecting superfluous forms of data in a potentially invasive way (i.e., ambient listening).

4.6.1 Privacy Control. A one-way MANOVA comparing Intention to Continue Use, Perceived Data Literacy, Affective Discomfort, and Ambivalence Toward Data Practices between the AT versions with and without Privacy Control provided no statistically significant results (Pillai's trace = 0.006, $F(1, 203) = 0.30$, $p = 0.88$). The lack of a difference suggests that, counterintuitively, the presence of Privacy Control might have little influence when invasive data practices are ambiguous.

4.6.2 Intention to Continue Use. The MLR model for examining how the Intention to Continue Use of Remember Music when it is ambiguously threatening is collectively influenced by the various factors mentioned above accounted for 42% of the variance (adjusted $R^2 = 0.42$, $F(10, 193) = 15.88$, $p < 0.001$).

As Table 4 shows, the Intention to Continue Use of the app exhibited three statistically significant main effects: Perceived Data Literacy ($\beta = 0.48, p < 0.001$), Perceived Realism of Data Practices ($\beta = 0.24, p = 0.004$), and the Requirements subscale of the AIPC scale ($\beta = -0.22, p = 0.001$). Although the influence of the presence of Privacy Control was not statistically significant by itself, we found that the Intention to Continue Use of the app was influenced by an interaction effect between Privacy Control and Perceived Realism of Data Practices ($\beta = 0.17, p = 0.05$). By conducting a post hoc comparison of slopes, we found that Perceived Realism of Data Practices is positively associated with the presence of Privacy Control ($p = 0.05$). The interaction suggests that users seem to expect the provision of privacy control when it is difficult to determine whether vaguely-specified invasive data practices are realistic.

Similar to the other two treatments, we found that higher intention to use an ambiguously invasive app came with greater expectations for transparency and control regarding data practices (as measured by the Requirements subscale of the AIPC scale). In addition, the intention to use an ambiguously invasive app was higher for those who judged themselves to possess higher data literacy and expressed higher levels of belief that the potentially invasive data practices are a normal feature of typical real-world apps. As in the other treatments, it appears that people would continue to use an ambiguously invasive app if the data practices that make the app creepy are realistic and believed to be understood. However, unlike in the other two variations of the treatment, when ambiguously invasive data practices were deemed realistic, affective discomfort was apparently not enough to deter participants from using an app that employs such practices. In essence, when people expect apps to be creepy, they are likely to be inclined to use creepy apps.

4.7 Summary of Findings

We summarize the results of the above analyses by revisiting the four hypotheses we formulated in Section 2 and addressing the two research questions we presented in Section 1.

4.7.1 Hypotheses. When examined separately, the presence of Privacy Control was positively associated with the Intention to Continue Use of Remember Music. However, when considered alongside other relevant factors, Privacy Control was generally unrelated to the Intention to Continue Use of the app. Therefore, we *reject* H1: "The perceived presence of privacy control is associated with increased intention to continue using a privacy-invasive app." In all study conditions, we found Perceived Data Literacy to be positively associated with the Intention to Continue Use of Remember Music, leading us to *accept* H2: "Perceived data literacy is positively associated with the intention to continue using a privacy-invasive app." Affective Discomfort was negatively associated with the Intention to Continue Use of Remember Music, but only in the VE and PB treatments. We therefore *partially accept* H3: "Affective discomfort is negatively associated with the intention to continue using a privacy-invasive app." Similarly, Ambivalence Toward Data Practices of Remember Music was positively associated with the Intention to Continue Use of the app only in the VE and PB treatments. Therefore, we *partially accept* H4: "Ambivalence toward the data practices of a privacy-invasive app is positively associated with the intention to continue using the app."

4.7.2 RQ1. Our findings indicate that the presence of privacy control is associated with a greater intention to use privacy-invasive apps, but only when privacy control is examined by itself. When considered in concert with other relevant factors, including data literacy and views regarding data practices of the app, the influence of privacy control is nullified. This finding appears to align with Solove's [63] problems with the logic of the privacy paradox.

4.7.3 RQ2. We found that affective discomfort can have a negative relationship with people's intentions to use privacy-invasive apps. However, the relationship may be tempered or nullified by other factors, such as ambivalence toward potentially invasive data practices of the apps, ambiguity regarding privacy threats, and alignment with data practices expected from typical real-world apps. In particular, when ambiguous data practices of an app are considered to align with how apps used in everyday life are expected to operate, affective discomfort does not seem to dissuade people from continuing to use the app.

5 DISCUSSION

Building upon prior literature in the emerging domain of affective privacy (e.g., [58, 61, 67]), the findings we described above highlight the importance of affect in privacy-related user decisions. More than that, the findings of our study highlight the need to take affect more seriously within privacy studies writ large. Our earlier work [58] has demonstrated that people do not feel adequately empowered to manage their privacy because the greater context of infrastructures, social norms and expectations, and technologies systematically disempowers users. Indeed, through perceived or experienced lack of empowerment, people routinely feel resigned to expect and accept privacy violations. In the context of apps, privacy control is constrained by systems of 'power over' that limit people's capacity to act in meaningful ways. People's experiences of such constraints are necessarily affective.

Nussbaum [46] has highlighted the relevance of affect to understanding the experience of everyday life:

> Given a deep attachment to something outside one's own control, the very accidents of life, combined with that attachment to an object, will bring the person who is so attached now into intense joy, when the beloved object is at hand, now into fear, when it is threatened, and now into grief, when catastrophe befalls it [46, p. 87].

The dynamics of emotional states and their relationship to objects and events described by Nussbaum highlight the general relevance of affect – affective discomfort, in particular – to the study of digital privacy. When people become attached to data-hungry apps and experience them as objects integral to practices of daily life, such relevance extends to privacy-related user experiences, particularly when privacy is fundamentally understood as a problem of control (cf. [78]). After all, user experience may be readily reduced to the efficient interaction of thumbs, eyes, and screens, but it is just as readily framed as a building block of daily life. If apps are ubiquitous, then their ubiquity forms part of the context of experiencing everyday life. When data privacy is predominantly characterized as a problem of control [78] (i.e., the control over one's data despite the unequal distribution of power between platforms and users [58]), routinized privacy violations lead to shaded facets of what Nussbaum refers to as "despair" [46].

Catastrophes [46] and violations of the expected functionality of daily infrastructures [57] do not become less catastrophic or problematic upon regular repetition, but become *normalized*. While our findings present evidence of such normalization, anecdotal evidence points to the use of 'creepy' as a buzzword for the nebulous push-and-pull between consumer-driven convenience and dubious data practices.[2] Such buzzword status highlights the salience of the concept of creepiness in the social imaginary [71] of users and speaks to the ongoing affectively catastrophic experience of privacy: the contention between social norms, data practices, and the people who live between the two.

We contend that the normalization of affective discomfort is a symptom of continued catastrophic failure in an infrastructural sense [66] such that the infrastructure and its users become distinctly visible [57]. Such visibility takes the form of emotional reaction that should be an integral aspect of the discourse of privacy. By presenting evidence of the normalization of affective discomfort, we extend our previous work [58] on the affective experience of (dis)empowerment when using apps.

The participants in our study knew how to act when Remember Music violated their expectations in ways they typically encounter when using other apps. For instance, when Remember Music violated expectations by collecting common but superfluous forms of data (e.g., location in the VE treatments), participants indicated not only that they understood what the app was doing with their data, but that such data practices were realistic. When the app breached their personal boundaries by communicating data to their social

[2] See, for example: https://foundation.mozilla.org/en/privacynotincluded/.

networks (as in the PB treatments), participants responded similarly. Indeed, in the VE and PB treatments, greater ambivalence toward data practices was associated with greater intention to continue using Remember Music. Such a relationship between ambivalence and use may be one of the mechanisms by which affective discomfort related to privacy-invasive apps is normalized: 'when ambivalent, just use the app.' When people default to using an app even when they are ambivalent toward its potentially invasive data practices, they, perhaps inadvertently, legitimize the practices, leading to their subsequent normalization *through use*.

However, the relationship between ambivalence and intention to use privacy-invasive apps does not hold when potentially invasive data practices are ambiguous, as was the case in the AT treatments. In such cases, the intention to use privacy-invasive apps seems to be driven by whether the invasive data practices align with people's routine experiences with the data practices of typical real-world apps. When the user experience of privacy is cloaked in the affective discomfort of broken promises [47], affective discomfort as a 'normal' aspect of app use becomes a self-fulfilling prophecy.

As noted above, the intention to use a privacy-invasive app is positively associated with ambivalence toward its data practices as well as with a match between the data practices and those expected of typical real-world apps. The relationships of the intention to use the app with these two factors may help resolve the privacy paradox. People deem privacy as important and voice their concerns regarding privacy violations, but the normalization of privacy-invasive data practices leads them to resign themselves to putting up with such violations. Creepy data practices normalize the expectation that affective discomfort is part and parcel of using apps; tolerating them further normalizes such experiences.

The identification of a normalized state of affective discomfort challenges the success and validity of prior work intended to design *around* creepiness [82]. Users may experience affective discomfort in the form of creepiness when they engage with an avatar who has an unexpected number of fingers [56] or when Alexa whispers to them [48]. These forms of creepiness may be designed around, as demonstrated by the typical HCI approach to develop designs that reduce creepy user experiences. However, such an approach treats creepiness as a "human factor" to be designed around, rather than as an essential human experience. Not all affective discomfort is created equal, nor can the many facets of affective discomfort be reduced to creepiness. Locating affective discomfort in aesthetic and sensory characteristics of technology (cf. [82]) reveals only part of a larger conceptual structure. The revealed part might just be the tip of an iceberg. The search for what lies beneath requires treating creepiness as a pivotal concept for developing fundamental knowledge about the relationship between the affective conditions of human life in a world that is changing rapidly through technological proliferation.

6 IMPLICATIONS

When affective discomfort is a normalized aspect of app use and app use continues to proliferate and mediate aspects of daily life, the use of apps becomes a fundamentally humanistic concern. Ten years from the initial discussions of creepiness within the privacy community [73] and twenty years from the first modern discussion of the privacy paradox [16], it is time to take affective discomfort seriously – not merely as something to be designed around based on the visual appearances of a given technology [82], but as a harbinger of sociotechnical conditions to come. With its profound interdisciplinarity, the HCI community is ideally positioned to tackle this truly human-centered problem.

Since HCI is historically grounded in improving human-computer interaction (or addressing human factors in computing), part of its agenda is predicated on the success of computing. It is reasonable to expect that HCI scholarship will contribute to the computer reaching out [10, 25]. The computer not only reaches out [25], but it is often "pushed out" by HCI researchers [10, 11]. The apparent normalization of affective discomfort identifies an overlooked vector of this reaching/pushing out process. As computing has become ubiquitous, apps and platforms shape implicit expectations of daily life [71], including but not limited to one's affective experiences [58, 61, 67] that tint and temper such expectations [57].

Discussion of user experience in HCI often implicitly draws upon a long lineage of work that situates it in the direct relationship between a user and a device (e.g., [22]). The logic is that better user experiences foster increased use. When user experience is operationalized, either implicitly or explicitly, as existing within the well-defined dyad of user and device [22], solutions to undesirable experiences are logically situated within the same dyad. For instance, calling creepiness out as a function of aesthetics [82] serves to focus design efforts on the aesthetics alone, typically overlooking the broader human experience of being a user in an increasingly digitized world. Such solutions solve problems of privacy for the *user* rather than the *human*.

With mounting evidence that cognitive and affective factors contribute to the normalization of creepiness when using apps, we assert that approaches to developing privacy solutions that rely on users as perfectly rational actors are not sufficient. For instance, mechanisms for privacy control appear as solutions only when the problem to be solved is located at the small scale of user and device. Such 'solutions' may reduce the complexity of the problem of privacy to a manageable form, but the reduction fails to account for the scale of literal *human*-computer interaction or the affective effects of such scaling, such as the normalization of affective discomfort. Failing to address the normalization of affective discomfort perpetuates the associated conditions of exploitation and legitimizes invasive data practices that are detrimental to the dignity of *people*. Our findings make the case for the HCI privacy community to move beyond the development of solutions for the reductive and non-scalable relationship between an individual user and an individual app.

The human in 'human-centered computing' should be understood as more than a mere user. Users are *people*, too. People *feel* as much, if not more, than they *think*. Humans are affective and experiential agents. Genuinely human-centered solutions must account for affective human experiences in order to address the user experience of affective discomfort. Focusing on affective discomfort, enables, even obligates, researchers and practitioners not to be overly conservative in operationalization of 'user experience,' particularly as it relates to data practices.

We contend that treating affective discomfort that results from entrenched data practices as a fundamental aspect of the experience

of the user as a human requires scaling beyond the point where the thumb meets the screen and accounting for the broader sociotechnical landscape within which the data practices are embedded. It is one thing to study affective discomfort when only a small set of users are creeped out or creepiness is relegated to highly specific interactions. It is another thing entirely to attempt to scale that study to a widespread phenomenon which necessarily involves *every* app that collects and uses data. It is yet another thing, still, to continue focusing on a paradox that might not be paradoxical at all when accounting for the role of affect in motivating user decisions.

7 LIMITATIONS

The generalizability of our findings may be affected by the standard limitations of self-reporting and self-selection. To control for the impact of cultural influences, we restricted participation to AMT workers from the United States. While the AMT population is a suitable proxy for studying Americans between the ages of 18 and 50 who have at least some college education, it is not necessarily representative of the general population of the United States [52]. Therefore, studies with additional samples are needed to verify generalizability to the United States and other regions. Similarly, generalizability of the findings to types of apps other than the one we depicted in the scenarios requires verification. We further point out that normalization is a temporal process that happens at long intervals. Longitudinal investigations could provide additional meaningful insight on temporal patterns.

While we made no gender-specific directional hypotheses, we investigated the potential relevance of gender to our research questions by including it as an exploratory variable in our models. We adhered to the best practices of inclusivity [70] when collecting data on participant gender. Two participants in our sample (0.3%) self-identified as non-binary, roughly in line with the relatively small proportion of non-binary individuals in the adult US population (0.5%) [79]. While keeping the tiny proportion of non-binary responses would not have had a meaningful impact on the overall results of other statistical analyses, low membership numbers in the third level of the gender variable were statistically non-usable and would have precluded us from examining the impact of gender. Therefore, we needed to set aside the data from the two non-binary participants despite our commitment to inclusivity in research. Our experience calls for greater attention to the development of methods that can be effective for the inclusion of disproportionately smaller groups in research on privacy and other areas of HCI.

8 CONCLUSION

We investigated why people continue to use apps they consider to be creepy. When examined separately, privacy control appears to account for people's use of an app which employs privacy-invasive data practices that they find to be creepy. However, when considering multiple relevant factors connected to people's intention to use a privacy-invasive app, we found that the influence of privacy control disappears. Instead, intention to use an app despite finding it creepy can be explained better by considering *affect*. Our findings demonstrate that affectively discomfiting user experiences have become normalized aspects of app use driven by entrenched privacy-invasive data practices. Treating users as affective agents and accounting for the broader sociotechnical landscape within which the data practices are embedded is therefore essential for developing privacy-related user experiences that respect the data and dignity of people as humans, not merely users. Efforts to humanize the user by focusing on affect can yield meaningful insight into persistent problems at the intersection of privacy and HCI.

ACKNOWLEDGMENTS

We thank the study participants for their time and effort. We are grateful to the anonymous reviewers whose feedback helped improve the paper. We acknowledge the Center of Excellence for Women & Technology at Indiana University Bloomington for enabling Emily Swiatek's participation in the research. The research described in this paper is partially supported by a grant (#CNS-1845626) from the National Science Foundation (NSF). The contents of the paper are the work of the authors and do not necessarily reflect the views of the sponsors.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.1126/science.aaa1465

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758. https://doi.org/10.1002/jcpy.1191

[3] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[4] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The Economics of Privacy. *Journal of Economic Literature* 54, 2 (June 2016), 442–92. https://doi.org/10.1257/jel.54.2.442

[5] Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt. 2021. Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 68, 13 pages. https://doi.org/10.1145/3411764.3445677

[6] Hunt Allcott and Matthew Gentzkow. 2017. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives* 31, 2 (May 2017), 211–236. https://doi.org/10.1257/jep.31.2.211

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

[8] Sarah Anrijs, Koen Ponnet, and Lieven De Marez. 2020. Development and Psychometric Properties of the Digital Difficulties Scale (DDS): An Instrument to Measure who is Disadvantaged to Fulfill Basic Needs by Experiencing Difficulties in Using a Smartphone or Computer. *PLOS ONE* 15, 5 (2020), 15 pages. https://doi.org/10.1371/journal.pone.0233891

[9] Sara Bannerman. 2019. Relational privacy and the networked governance of the self. *Information, Communication & Society* 22, 14 (2019), 2187–2202. https://doi.org/10.1080/1369118X.2018.1478982

[10] Jeffrey Bardzell and Shaowen Bardzell. 2015. Humanistic HCI. *Synthesis Lectures on Human-Centered Informatics* 8, 4 (Sep 2015), 1–185.

[11] Jeffrey Bardzell and Shaowen Bardzell. 2016. Humanistic HCI. *Interactions* 23, 2 (Feb 2016), 20–29. https://doi.org/10.1145/2888576

[12] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. In *2006 IEEE Security and Privacy (IEEE S&P 2006)*. Oakland, California, 15 pages. https://doi.org/10.1109/SP.2006.32

[13] Susanne Barth and Menno D. T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

[14] 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. https://doi.org/10.1177/1948550612455931

[15] Kimberly A. Brink, Kurt Gray, and Henry M. Wellman. 2019. Creepiness Creeps In: Uncanny Valley Feelings Are Acquired in Childhood. *Child Development* 90, 4 (2019), 1202–1214. https://doi.org/10.1111/cdev.12999

[16] Barry Brown. 2001. *Studying the Internet Experience*. Technical Report HPL-2001-49. HP Laboratories Bristol. http://www.hpl.hp.com/techreports/2001/HPL-2001-

[61] 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
[62] Daniel J. Solove. 2012. Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126, 7 (2012), 1880–1903.
[63] Daniel J. Solove. 2021. The Myth of the Privacy Paradox. *George Washington Law Review* 89, 1 (2021), 1–51.
[64] Sowmya Somanath, Ehud Sharlin, and Mario Costa Sousa. 2013. Integrating a robot in a tabletop reservoir engineering application. In *8th ACM/IEEE International Conference on Human-Robot Interaction (HRI 2013)*. 229–230. https://doi.org/10.1109/HRI.2013.6483585
[65] 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
[66] Susan Leigh Star and Karen Ruhleder. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research* 7, 1 (1996), 111–134. https://doi.org/10.1287/isre.7.1.111
[67] Luke Stark. 2016. The emotional context of information privacy. *The Information Society* 32, 1 (2016), 14–27. https://doi.org/10.1080/01972243.2015.1107167
[68] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. 2016. Bridging the Gap between Privacy by Design and Privacy in Practice. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 3415–3422. https://doi.org/10.1145/2851581.2856503
[69] Arlonda Stevens and Casey Newmeyer. 2017. Creepy and intrusive: A consumer's perspective of online personalized communications. In *Contemporary Issues in Social Media Marketing*. Routledge, Milton Park, UK, 172–183.
[70] Simone Stumpf, Anicia Peters, Shaowen Bardzell, Margaret Burnett, Daniela Busse, Jessica Cauchard, and Elizabeth Churchill. 2020. Gender-Inclusive HCI Research and Design: A Conceptual Review. *Foundations and Trends in Human-Computer Interaction* 13, 1 (March 2020), 1–69. https://doi.org/10.1561/1100000056
[71] Charles Taylor. 2002. Modern social imaginaries. *Public Culture* 14, 1 (2002), 91–124. https://muse.jhu.edu/article/26276
[72] Omer Tene and Jules Polonetsky. 2013. A Theory of Creepy: Technology, Privacy and Shifting Social Norms. *Yale Journal of Law and Technology* 16 (2013), 59–102.
[73] 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
[74] David Vincent. 2016. *Privacy: A Short History*. Polity Press, Malden, MA, USA.
[75] Paul Virilio. 2007. *The Original Accident*. Polity Press, Malden, MA, USA.
[76] Jeffrey Warshaw, Tara Matthews, Steve Whittaker, Chris Kau, Mateo Bengualid, and Barton A. Smith. 2015. Can an Algorithm Know the "Real You"? Understanding People's Reactions to Hyper-Personal Analytics Systems. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 797–806. https://doi.org/10.1145/2702123.2702274
[77] Margo C. Watt, Rebecca A. Maitland, and Catherine E. Gallagher. 2017. A case of the "heeby jeebies": An examination of intuitive judgements of "creepiness". *Canadian Journal of Behavioural Science / Revue canadienne des sciences du comportement* 49, 1 (2017), 58–69. https://doi.org/10.1037/cbs0000066
[78] Alan F. Westin. 1967. *Privacy and Freedom*. Atheneum Books, New York, NY, USA.
[79] Bianca D. M. Wilson and Ilan H. Meyer. 2021. Nonbinary LGBTQ Adults in the United States. The Williams Institute, Los Angeles, CA, USA. https://williamsinstitute.law.ucla.edu/wp-content/uploads/Nonbinary-LGBTQ-Adults-Jun-2021.pdf
[80] Richmond Y. Wong, Deirdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 111 (Dec 2017), 26 pages. https://doi.org/10.1145/3134746
[81] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a Privacy Fundamentalist Sell Their DNA for $1000…If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 1–18. https://www.usenix.org/conference/soups2014/proceedings/presentation/woodruff
[82] Paweł W. Woźniak, Jakob Karolus, Florian Lang, Caroline Eckerth, Johannes Schöning, Yvonne Rogers, and Jasmin Niess. 2021. Creepy Technology: What Is It and How Do You Measure It?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 719, 13 pages. https://doi.org/10.1145/3411764.3445299
[83] Heng Xu, Xin (Robert) Luo, John M. Carroll, and Mary Beth Rosson. 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems* 51, 1 (2011), 42–52. https://doi.org/10.1016/j.dss.2010.11.017
[84] 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*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300303
[85] 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

APPENDICES

A SCENARIO TEXT

Each study condition included the text of the core scenario. In the control condition, no additional information was included. In the treatment conditions, we provided additional text corresponding to the treatment.

A.1 Control (Core Scenario)

Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.

A.2 Violation of Expectations (VE)

A.2.1 **Privacy Control (VE/C).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT]
Today, you received an email from Remember Music recommending songs that 'your neighbors and people near you are listening to now.' You were not aware that the app used location data. You navigate to Remember Music's settings on your phone and find a tab called 'Location Data.' Preferences within this tab allow you to prevent the app from using your location data to share with others what you are listening to now. You prevent the app from using your location and receive a confirmation that your preferences have changed.

A.2.2 **NO Privacy Control (VE/NC).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT] Today, you received an email from Remember Music recommending songs that 'your neighbors and people near you are listening to now.' You were not aware that the app used location data. You can't find a way to change Remember Music's access to your location data.

A.3 Breach of Personal Boundaries (PB)

A.3.1 **Privacy Control (PB/C).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT]
Today, when you opened your social media account, you saw that Remember Music has inserted a publicly visible sidebar on your profile that allows your social network to see your music listening history. In your case, it includes several graphic images associated with some of the songs in your listening history. You don't want your coworkers and family to see these images. You navigate to Remember Music's settings on your phone and find that you can turn off social media data sharing. After selecting that option, you navigate back to your social media page, and the Remember Music sidebar is gone. You receive a confirmation that your preferences have changed.

A.3.2 **NO Privacy Control (PB/NC).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT]
Today, when you opened your social media account, you saw that Remember Music has inserted a publicly visible sidebar on your profile that allows your social network to see your music listening history. In your case, it includes several graphic images associated with some of the songs in your listening history. You don't want your coworkers and family to see these images, but you can't find a way to change Remember Music's social media sharing settings.

A.4 Ambiguity of Threat (AT)

A.4.1 **Privacy Control (AT/C).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT]
Remember Music informs you that 'an artist you have been interested in lately will be playing nearby.' You have been talking with your partner a lot about the artist, but you haven't used Remember Music to search for songs by the artist. You do not know how or why you received this recommendation. You navigate to Remember Music's settings on your phone, where you find a description of the app's data-sharing practices. You do not recall opting in to receive this type of notification, but easily identify how to opt out. You receive a confirmation that you will no longer receive recommendations for concerts in your area.

A.4.2 **NO Privacy Control (AT/NC).**

[CORE SCENARIO]
Last week while you were streaming a show, you heard a new song that you really liked. You couldn't identify the song despite searching for it online. So you decided to download an app called Remember Music that uses your phone's microphone to identify songs. You installed the app, clicked through the user agreement, re-streamed the show, and used the app's 'listen' function to identify the song. The app quickly returned the artist and the song title along with ads from third parties targeted specifically to your interests. You started using the app whenever you heard a new song you liked.
[ADDITIONAL TEXT FOR TREATMENT]
Remember Music informs you that 'an artist you have been interested in lately will be playing nearby.' You have been talking with your partner a lot about the artist, but you haven't used Remember Music to search for songs by the artist. You do not know how or why you received this recommendation.

B QUESTIONNAIRE

B.1 Commitment Question

We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in this study.

Will you provide your best answers to each question in this study?

- ○ I will provide my best answers.
- ○ I will not provide my best answers.
- ○ I cannot promise either way.

B.2 Scenario

In the first section of this questionnaire, you will be presented with a scenario about a music app. Please read this scenario carefully and indicate your level of agreement with each statement that follows it.
[Text of the scenario corresponding to the randomly-assigned study condition.]

B.3 Scenario Reading Check

What is the name of the app described in the scenario you read?
[NOTE: The items below were presented in random order.]

- ○ Music for You
- ○ Remember Music
- ○ Listening Always
- ○ Music App
- ○ I am not sure.

B.4 Affective Perceptions

Please indicate the extent to which you agree with the following statements:
(Options: Strongly agree, Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree, Strongly disagree)
[NOTE: The items below were presented in random order.]

- I have a feeling that there is something shady about Remember Music.
- I think the Remember Music app is creepy.
- I expect complications when I start using Remember Music.
- I think the way Remember Music uses my data is absurd.
- I understand what kinds of data Remember Music collects.
- I would be comfortable with the way Remember Music uses my data.
- I would continue to use Remember Music based on the scenario.
- I understand how Remember Music uses the data it collects.
- I think the manner in which Remember Music uses my data is realistic.
- I do not know how to feel about how Remember Music uses my data.

[NOTE: The following item was included among the above items as an ATTENTION CHECK:
Please select 'Somewhat disagree' in response to this item to show that you are reading carefully.]

B.5 AIPC Scale

We would like to know a bit about your general attitude regarding various technological matters.
Please indicate the extent to which you agree with the following statements:
(Options: Strongly agree, Agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Disagree, Strongly disagree)
[NOTE: The items below were presented without the subscale information. The subscales are included below only for informational purposes.]

- Mobile app privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. [REQUIREMENTS subscale]
- Control of personal information lies at the heart of mobile app users' privacy. [REQUIREMENTS subscale]
- I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want. [ANXIETY subscale]
- I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy. [ANXIETY subscale]
- Mobile app providers seeking information online should disclose the way the data are collected, processed, and used. [REQUIREMENTS subscale]
- A good privacy policy for mobile app users should have a clear and conspicuous disclosure. [REQUIREMENTS subscale]
- It is very important to me that I am aware and knowledgeable about how my personal information will be used. [PERSONAL ATTITUDES subscale]
- I am concerned that mobile apps may monitor my activities on my mobile device. [ANXIETY subscale]
- I am concerned that mobile apps are collecting too much information about me. [ANXIETY subscale]
- I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization. [ANXIETY subscale]
- When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes. [ANXIETY subscale]
- I am concerned that mobile apps may share my personal information with other entities without getting my authorization. [ANXIETY subscale]
- Compared to others, I am more sensitive about the way mobile app providers handle my personal information. [PERSONAL ATTITUDES subscale]
- To me, it is the most important thing to keep my privacy intact from app providers. [PERSONAL ATTITUDES subscale]
- I am concerned about threats to my personal privacy today. [ANXIETY subscale]

[NOTE: The following item was included within the above items as an ATTENTION CHECK:
Please select 'Somewhat agree' in response to this item to show that you are reading carefully.]

B.6 General Technical Expertise Subscale of the Digital Difficulties Scale

Please indicate the extent to which you agree with the following statements:
(Options: Agree, Rather agree, Neither agree nor disagree, Rather disagree, Disagree)

- In general, I often have difficulty when using my smartphone, apps, websites, or computer programs.
- In general, I am not able to solve questions or problems on my own when using my smartphone, apps, websites, or computer programs.
- In general, I need support when trying out something new on my smartphone or computer.
- In general, I find it hard to adjust settings of my smartphone, apps, websites, or computer programs (for example, privacy or safety settings).
- In general, I often have questions or problems when using my smartphone, apps, websites, or computer programs after an update has been done.

B.7 Technology Use

Now, we would like to know about your personal technology use.

- What is the operating system of your smartphone?
  - ○ iOS (i.e., Apple)
  - ○ Android
  - ○ Something else. Please specify: [text box]
- How often do you change privacy settings or permissions for apps on your smartphone?
  - ○ Daily
  - ○ Once a week
  - ○ Twice a month
  - ○ Monthly
  - ○ Every other month
  - ○ Never
  - ○ I don't know
- Approximately how many apps do you have on your smartphone?
  - ○ 1–10
  - ○ 11–20
  - ○ 21–30
  - ○ 31–40
  - ○ 41–50
  - ○ More than 50
  - ○ I don't know

B.8 Demographics

Finally, tell us a little bit about yourself.

- What is your year of birth?
  [dropdown of years from 2010 to 1920]
- What is your gender?
  - ○ Woman
  - ○ Man
  - ○ Non-Binary
  - ○ Prefer not to disclose
  - ○ Prefer to self-describe: [text box]
- What is your ethnic background? *(Select all that apply.)*
  - □ African American / Black
  - □ Native American
  - □ Asian
  - □ Caucasian / White
  - □ Hispanic / Latino
  - □ Pacific Islander or Native Hawaiian
  - □ Prefer not to say
  - □ Something else. Please specify: [text box]
- What is the number between two and four?
  [ATTENTION CHECK]
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ 5
  - ○ 6
  - ○ 7
- Are you a student?
  - ○ Yes
  - ○ No
- If 'Yes' is selected for the question "Are you a student?" then ask:
  What is your field of study? [text box]
- What is the highest level of education you have completed? (If currently enrolled, highest degree received.)
  - ○ Less than high school
  - ○ High school graduate
  - ○ High school equivalent
  - ○ Vocational training
  - ○ Some college
  - ○ College graduate (B.S., B.A, or other 4-year degree)
  - ○ Master's degree
  - ○ Doctoral degree
  - ○ Professional degree (e.g., MD, JD)
  - ○ Prefer not to say
  - ○ Something else. Please specify: [text box]
- What is your current employment status? *(Select all that apply.)*
  - □ Employed full-time
  - □ Employed part-time
  - □ Unemployed looking for work
  - □ Unemployed not looking for work
  - □ Homemaker
  - □ Student
  - □ Retired
  - □ Disabled
  - □ Prefer not to say
  - □ Something else. Please specify: [text box]
- If 'Employed full-time' or 'Employed part-time' is selected for the question "What is your current employment status?" then ask:
  What is your occupation? [text box]

- How many years have you lived in the United States?
  - 1
  - 2
  - 3
  - 4
  - 5
  - 6
  - 7
  - 8
  - 9
  - 10
  - More than 10
  - All my life
- What is your annual household income?
  - Less than $10,000
  - $10,000 - $19,999
  - $20,000 - $29,999
  - $30,000 - $39,999
  - $40,000 - $49,999
  - $50,000 - $59,999
  - $60,000 - $69,999
  - $70,000 - $79,999
  - $80,000 - $89,999
  - $90,000 - $99,999
  - $100,000 - $149,999
  - More than $150,000
  - Prefer not to say
- Which of the following best describes the locality where you live?
  - Urban
  - Suburban
  - Rural
- Is there anything else you'd like to tell us?
  [essay-type text box]