Exploring Users' Perspectives of Mobile Health Privacy and Autonomy

Thomas Starks(✉), Kshitij Patil, and Aqueasha Martin-Hammond

School of Informatics, Computing, and Engineering, Indiana University – Indianapolis, Indianapolis, IN 46202, USA
{tmstarks,kshpatil,aqumarti}@iu.edu

Abstract. The increased use of mobile health (mHealth) applications and the corresponding exchange of sensitive data has underscored privacy concerns. Privacy notices are often unengaging or incomprehensible, leading to questions of informed consent and trust. While studies have focused on providing solutions aimed to simplify privacy language and reduce cognitive burden, often overlooked are the behavioral aspects of individual attitudes, norms, and perceived control that lead to dynamic intentions for engagement. In this paper, we use existing behavior models as a lens to understand users' privacy experiences, behaviors, and perspectives toward mHealth data privacy policies. In 15 semi-structured interviews with adult users of mHealth applications, participants encountered persistent challenges when engaging and articulating the value of privacy. Participants do not understand how privacy notices are designed, which leads to superficial awareness and control that does not actually support their perceptions of autonomy and trust in mHealth. As a result, users felt sub-optimal autonomy when engaging in privacy interactions. We discuss design considerations for autonomy-supporting privacy notices that may help users feel a greater sense of agency when interacting with mHealth applications.

Keywords: Human-centered computing · Human computer interaction (HCI) · Empirical studies in HCI · Security and privacy · Human and societal aspects of security and privacy · Usability in security and privacy First Section

1 Introduction

Technology-driven health solutions such as mHealth applications are both prolific and challenging for privacy policy researchers, designers, and practitioners. mHealth applications are categorized as any mobile device that captures and obtains health-related data to improve quality-of-care (Cameron et al. 2017), which span diabetes management, sleep, medication, and general health and wellness, among others. The data accompanying mHealth applications require privacy policy designers to consider both regulatory compliance and individual privacy behaviors when crafting user policies, frameworks and solutions that meet privacy goals. For example, privacy design research has shown

D. Salvi et al. (Eds.): PH 2023, LNICST 572, pp. 70–91, 2024.
https://doi.org/10.1007/978-3-031-59717-6_5

promising results for reducing users' cognitive load through limiting excessive reading and decreasing users' burden through design considerations (Schaub et al., 2017). mHealth privacy research has also examined consumer's abilities to consent to data practices, such as how their data is used and stored, which is a core component of Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and the Common Rule, three regulations that regulate the processing of personal data, outline provisions of human subject research, and safeguards privacy of medical data and other personal data (Nurgalieva et al., (2020), Arora et al., (2014)). Practitioners have also explored technical solutions that improve users' privacy awareness and ability to comply with regulatory requirements (i.e., GDPR and HIPAA) (Iwaya et al., 2022). Yet, oftentimes existing practices and approaches emphasize obtaining consent, sometimes neglecting that people ignore, or fail to understand the risks and implications of using an application or their participation in its data usage (Degeling et al., (2018), Schaub et al., (2017)). Therefore, users are often faced with the classic tradeoff between application (i.e., app) utility and privacy which ultimately leads to a black box where users are not fully informed about their data privacy rights. This presents a chasm for users and privacy policy designers positioned at the intersection of legal compliance and usable privacy design.

The rapid emergence of connected mHealth solutions has enabled more personalized and informed care (Steinhubl et al., 2015) but the ability to understand user attitudes and behaviors towards mHealth data privacy is a known trust-related barrier to user adoption (Lynch et al., (2017), "Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care", (2010), (Zou et al., 2020)) and remains a challenge. One open challenge is that these solutions often ignore other relevant factors such as dynamic intent or perceived control that might impact users' behaviors in the context of healthcare (Ruotsalainen et al., 2012). We must therefore further understand the factors beyond data control and consent that influence user behaviors in the mHealth context to identify appropriate opportunities and solutions to address users' needs when interacting with privacy policies. It is imperative to better understand the intricacies of individual data privacy behaviors when interacting with mHealth applications to derive further design considerations that can inform this ubiquitous and evolving data-driven environment of mHealth. We posit that user attitudes and behaviors have a deterministic contribution in helping to identify the strengths and limitations of current privacy policies that are designed to help motivate individual data privacy behaviors, engagement, and understanding.

In this paper, we investigate users' attitudes and self-reported behaviors when engaging with mHealth data privacy policies to understand context-specific factors and opportunities to improve mHealth privacy policy design. We conducted interviews with 15 adults that use mHealth applications to understand their attitudes and behaviors toward existing mHealth privacy policies, challenges, and opportunities for improvement of these policies. During interviews, we used a focused set of probes (Appendix Table 3) to support reflection when sharing their prior experiences with mHealth data privacy policies. We selected these applications because they covered broad reaching health domains ranging from wellness (i.e., sleep) to mission-critical healthcare management (i.e., diabetes care and medication adherence), which were believed to have unique elements in

data privacy decisions. In addition, we noticed that each probe, while having some common elements, had unique user interfaces from a visualization perspective. We found that certain themes were consistent with existing usable privacy research. We also found that users' sense of autonomy, perceived control and willingness (Deci et al., 2012) in mHealth privacy policy interactions were often influenced by factors other than available data control and consent. Our work builds on usable privacy and mHealth behavioral research by extending knowledge of factors that impact users' interactions with mHealth data policies. Our work extends prior research (Atienza et al., 2015) exploring users' attitudes and behaviors toward existing privacy policies. However, we focus in the context of mHealth data exploring users' experiences engaging with applications that collect their personal health information to support them in managing their health. Our work contributes to the broader research community by merging concepts of behavioral design and usable privacy to improve language understanding, and promote trust in this environment. Specifically, we extend prior research (Audie et al., 2015) that explores users' attitudes and behaviors toward existing privacy policies.

2 Related Work

We acknowledge a few foundational domains which foreground our work. We see an evolving data collection surge where emerging questions of privacy and trust ensue. We believe health data privacy is particularly relevant at this intersection of technology and ethics, and describe these domains in detail below.

2.1 Ethics on Privacy, Trust, and Technology Acceptance

Researchers in the field of ethics have considerably investigated privacy, trust, and acceptance. In a world where pervasive automation advances significantly, AI researchers have developed frameworks to optimize personal autonomy (Calvo et al., 2020) and foreground risks (Floridi et. al., 2018). Frameworks in this space consider privacy a pillar of ethical design and essential for technology acceptance, especially in the mHealth domain (Mantovani et.al., 2017). As such, privacy as a construct has a paramount position that does not only facilitate ethical AI, but also affects utility, control, trust, and acceptance goals. Researchers recognize the broad application of AI, but ethical design must establish privacy as a basic individual right that withstands the deliverance of evolving pervasive systems (Bartoletti, 2019). The reasons consumers have a strong affinity for privacy is due to several complex factors. Researchers know that variation in demographics such as age and the type of data collected (i.e., health) can either help or hurt the trust they have in a health technology, and ultimately its acceptance or adoption (Poyner et al., (2018), Schomakers et al., (2019), Wang et al., (2019), Martin-Hammond et al., (2019), Guo et al., (2016)). While significant work has been done to improve consumers' willingness to accept health technology, some experience a sense of fatalism that is perpetuated by the evolving health system they interact with (Joo et al., (2021)). This fatalism is a sign of migrating chasms between the nature of perceived privacy and the growth at which consumers are exposed to new health promotions. Researchers explore this intersection, but many do not entirely approach grounding health privacy

in a proactive tradition. It is no longer ethical to misconstrue preference and control as a sufficient end towards proactive privacy. Researchers enable preference selection and other usable privacy interactions as a means to promote control over one's health data, but control is only one variable that presupposes another integral and widely overlooked virtue of autonomy. It is this belief that motivates our work and distinguishes this research from others that focus on elderly populations (Detweiler et al., 2016). More specifically, the composition that makes up autonomy is not well understood and established within advancing interconnected health systems. We will further explore the topic in later sections.

2.2 Pervasive mHealth and Black Box Use Cases

Pervasive health through the use of sensor technology has generated broad and deep insights (Wang et al., 2022). Some mHealth sensing information architectures and functionality enable health interventions by leveraging behavioral change through different engagement techniques. Some features that drive engagement such as forums present unique privacy challenges as well (Danaher et al., 2015). Other applications such as virtual health communities' research has also explored the topic of privacy (Kordzadeh et al., 2017), yet much of this research focuses on supporting human-human communication rather than human-machine communication, which makes the domain unique. What makes this area of HCI unique is the Mobile health (mHealth) component, which is defined as, "the use of mobile devices to monitor or detect biological changes in the human body, while device management entities, such as hospitals, clinics, or service providers, collect data and use them for healthcare and health status improvement" (Park, 2016), and is similar to others' (Ruotsalainen et al., 2012) definition in the context of pervasive health. mHealth can also include self-reported health data provided by users through consumer-focused personal tracking and reporting applications (Radbron et al., 2019). Although the growing ubiquity of mHealth applications has seemingly large potential upside to improve health through innovative and connected solutions such as IoT (Bertino et al., 2016), researchers are faced with navigating the need for large amounts of data with the complex domain of opaque health privacy (Quinn et al., 2022). To this end, many mHealth technologies have the large upside potential to transform healthcare through integrated machine learning capabilities and artificial intelligence. Although many contributions have been made in this arena, health-related stigmas can influence privacy perceptions and perpetuate concerns of the technology's utility (Arora et al., 2014). Design for sharing behavioral data in social constructs as leverage of peer support for health monitoring; also establishes engagement with data privacy across a lifecycle as an interesting research avenue (Vilaza et al., 2019).

Even though policies such as HIPAA provide protections for personal health data, users often still have concerns about what data is collected about them and how it is used (Al Ameen, 2012). As such, researchers are exploring ways to reduce negative impacts and perceptions through contextualizing privacy concerns in this space (Ferreira et al., 2021). For example, some researchers note that some mHealth privacy concerns are associated with age and can be used to tailor mobile applications to these users (Ferreira et al., 2021). Significant work has been done to define regulatory frameworks and user constraints in IoT environments (Poyner et al., 2018). Other work by Irwin Altman

confirms that privacy is both dynamic and subjective, and is susceptible to change over time along with different contexts, which is the basis for Privacy Regulation Theory. Irwin theorizes privacy as the control and feedback over information flow, which our work expands; however, the framework produced focuses heavily on contextualizing health environment monitoring solutions rather than mobile health, which we posit has proximal differences in interpretation (Moncrieff et al., 2009).

To address black-box perceptions in pervasive health technology, designing for transparency and choice are important in passive data sharing to reduce privacy concerns. Current design is still only accounting for upfront choice and transparency, and little with how choice and engagement are actively managed after data is shared (Kolovson et al., 2020). Some researchers posit "…the crux of modern machine learning: the reliance on powerful but intrinsically opaque models. When applied to the healthcare domain, these models fail to meet the needs for transparency that their clinician and patient end-users require. We review the implications of this failure, and argue that opaque models (1) lack quality assurance, (2) fail to elicit trust, and (3) restrict physician-patient dialogue. We then discuss how upholding transparency in all aspects of model design and model validation can help ensure the reliability and success of medical AI…" this forms the basis for not just opaque AI models in healthcare but also opaque data journeys in mHealth (Quinn et al., 2022). While regulation may be the de facto standard for ensuring privacy between interoperable devices like fitness trackers and smartwatches, device requirements subject to FDA and HIPAA are not widely acknowledged due to lack of awareness and misidentifying medical device classifications (Motti, 2019).

2.3 Privacy Control Versus Autonomy

Often, privacy behaviors appear to be dictated by technology that simply aims to provide control(s); through this lens, we see a challenge in autonomy due to a lack of self-direction, identity, and intrinsic factors (Deci et al., 2012). However, based on Self-Determination Theory (SDT), the premise of true autonomy in this context is the feeling that one is both being in control and willing to engage in good privacy-preserving behaviors – simply, we must transcend from designing controls to designing autonomy. We posit that privacy-by-design is being challenged in unique ways due to the complexity of systems that collect, process, and maintain data. While regulations such as GDPR and HIPAA exist to govern data practices and have an important role (Premarathne et al., 2015), their principles are collectively reduced to compliance-centric models, which leaves little room to improve usable mechanisms beyond 'cookies' (Degeling et al., 2018) or other usable privacy mechanisms. It is for this reason that existing privacy-preserving infrastructures are not fully capable to keep up with the needs of consumer mHealth innovations. An example of this resides in the health IoT environment where consumers value privacy over novel utilities and feel the two are somehow negotiated against each other (Zou et al., 2020). Researchers have aimed to address problems that exist between humans and ubiquitous computing, but mobile health wearables and applications in particular, have unique challenges related to secure interoperability between devices, databases, and governing infrastructures, which have created negative privacy perceptions (Ometov et al., 2021). These perceptions are perpetuated by the advancing need to continuously collect sensing and individual data to generate insights (Ometov

et al., 2021). However, similar to research on mobile crowdsourcing and trust authentication, the collection and processing methods in this environment are inadequately expounded on, thus consumers are left with gaps in knowledge about their data journey and have seemingly limited trust in the wearables they use (Feng et al., 2018). While researchers explore trust and control in various privacy models, once mHealth devices begin to collect data, ultimately, users are therefore left with the belief that their data is shared in a black-box environment intended to capitalize on their use of the technology without providing sufficient awareness of their data integrity. In this research, we explore users' perceptions of privacy policies to uncover factors they perceive to influence their autonomy in privacy policy interactions beyond the existence of privacy control(s). By doing so, we aim to understand how user self-reported behaviors are influenced, or not, by their sense of perceived autonomy in those interactions and identify design considerations for future autonomy-preserving privacy interactions.

3 Methods

Our interviews aimed to answer the following research questions:

- RQ1: What are users' current experiences with mHealth privacy policies?
- RQ2: What are users' attitudes and behaviors toward privacy policies for mobile applications that collect and use personal health data and why?

3.1 Theoretical Framing

Because we wanted to understand users' behaviors when engaging with the design of privacy policies in mhealth applications, we initially started with the Fogg Behavior Model (FBM) to help frame questions in our study protocol because of its focus on user behavior and technology design (Fogg, 2009). Fogg's model describes that user behaviors can be influenced by recognizing user motivation and ability, and potentially designing triggers that characterize those relationships (Fogg, 2009). However, we later expanded our theoretical framing during the analysis phase after exploring the data and realizing that broader concepts were emerging related to the Theory of Reasoned Action (TRA). The TRA focuses on motivations such as intents and a person's ability to act or adapt to behaviors according to them (Fishbein, 1979). Within the TRA, humans are viewed as rational decision-makers that when faced with a decision of pros and cons, adequately weigh them consistently and predictably in accordance with the most optimal economic benefit (Fishbein, 1979) – this decision-making is similar to privacy calculus in our research context. We quickly realized through iterative thematic analysis that TRA would succumb to limitations about perceptions of user control, which is why we explored a similar model that allowed us to focus on that component of behavioral intent. To characterize the relationship between intention and behavior, the Theory of Planned Behavior (TPB) describes intentions as multi-faceted, which rely on perceived levels of individual behavioral control, subjective norms, and attitudes (Icek, 1991). These dimensions of intent are dynamic and inherently conflict with behavioral economics where decisions are considered rational and reliable. In our data, we began to see concerns emerging that were related to understanding health privacy language and subsequent

voluntary consent to its practices. While we used FBM to design our study, we framed our analysis through the TPB to understand participant's interactions with mHealth privacy and how it relates to perceived autonomy (see Appendix Table 4 for an overview of this methodological process).

3.2 Participants

Participants were recruited from a local community in the surrounding areas of a midwest city in the United States. They were required to be age 18 years or older, and be current users of mhealth applications and consent to privacy policies. We chose a broad age range and were not intending to compare differences based on demographics at this phase of research. No participants were excluded. Participants' ages ranged from 28–67 years old (Appendix Table 1). All participants had a smartphone or mobile phone with internet access. Participants ranged in mHealth usage and frequency of privacy notice engagements. Participants encountered the policies through a variety of devices including Apple Watch, IoMT (Internet of Medical Things), iPhone, Alexa, smart appliances, Electronic Medical Records (EMR), and Fitbits among others. To further understand participants' existing views on data and privacy, we also asked them to share what they felt data and privacy mean (Appendix Table 2).

3.3 Study Procedures

During each 60-min semi-structured interview, we asked participants about their experiences with privacy notices when using mobile applications including health related apps. Additionally, we shared with participants various mHealth privacy notice examples as probes (Appendix Table 3) to help participants reflect on their own encounters with mHealth privacy policies, their attitudes and behaviors toward them, and factors they felt influenced their attitudes and behaviors (Hutchinson et al., 2003). Finally, we asked participants to reflect on barriers and challenges they faced, if any, and to brainstorm ideas of how they feel one might improve interactions with privacy policies to improve their sense of autonomy when engaging. Each participant was asked to complete a demographic and background survey at the end of the study. These questions were gathered to understand participant characteristics and technology experiences. We conducted interviews until we stopped hearing and seeing new data (i.e., saturation) (Chun Tie et al., 2019). After completing all interviews, we began analysis of the data.

3.4 Data Analysis

We audio recorded all interviews and transcribed them prior to data analysis. We used thematic analysis situated in Grounded Theory (GT) to analyze our data. The GT research process consists of collecting qualitative data, inductively assigning codes to data to develop themes, comparing themes with external research, and building theory from these themes (Chun Tie et al., 2019). This inductive process considers data saturation and external research comparisons to iteratively refine codes and themes to support the theory (Chun Tie et al., 2019). Once we confirmed a level of support from existing literature, we generated a codebook to guide our deductive coding process.

Using the codebook, two researchers independently coded two of the transcripts to further refine the codebook and establish inter-rater reliability (McDonald et al., 2019) between the researchers. Inter-rater reliability was assessed to determine the likelihood that two independent reviews of the same participant transcript yield similar outcomes. Thus, we wanted to determine if the generated codes were interpreted similarly between independent reviewers. Pre-defined acceptance criteria for the reliability score was set at 80% or greater on an individual quotation level aligned with existing practice. The researchers defined rules prior to analysis, which established which transcripts would be coded; rationale supporting this decision was based on the participant's code distribution and nominal representation of educational background compared to other subjects (undergraduate degree). Of 41 codes and definitions, the inter-rater reliability score of 80% was exceeded after initial comparisons and a round of discussion to address agreements and disagreements. Once consensus was established, one researcher coded the entire subset of transcripts using the codebook.

4 Findings

We found a need for additional focus on autonomy in mHealth privacy interactions. Participants had mixed-attitudes about the value and usefulness of mhealth privacy policies. For instance, we found that subjective norms and perceived control (beyond actual data controls provided) uniquely contributed to users' sense of autonomy in interactions with mHealth privacy policies. Participants believed that these additional factors should be considered in privacy policy design to facilitate personalized, engaging, and meaningful interactions in highly dynamic mHealth privacy situations. Our results suggest that beyond the ability to control personal data, users' sense of autonomy in privacy interactions may also rely on the ability of designers to truly engage users to understand how the design of solutions are intended to protect them. In the following subsections, we present results of what participants told us about their unmet needs for autonomy with mHealth privacy interactions.

4.1 Incongruent Informed Consent is a Barrier to Engagement and Trust

We learned that participants felt they often had to consent to mHealth privacy policies without being fully informed about them. Participants did not attribute this problem to a lack of information, but rather the question of what it means to be "informed" and how the information presented (with the goal of informing) engages the user. For example, P14 explained consent is often a binary choice but emphasized the distinction between consenting and being informed. They stated, "Theoretically, yes…if it comes down to that binary choice and if the consumer is being informed, then that's consent. If you're signing up for something and you're not being informed, that's not informed consent. So that's a different argument and that's a different situation…" So, while participants mentioned a lack of engagement with policy information, they also challenged the notion that listing information in a policy is sufficient for engaging users and helping them understand its meaning.

Participants also encountered situations where they lacked understanding of the information presented but felt obligated to consent in order to access the services. For example,

P10 stated, "It [consent] is definitely a gray area because technically by the book I am checking the box that I read and understand the notice. But if that is the only way that I'm going to be able to use this system [a mHealth system] that I want to use, there's not really much of an option for me to get further clarification or additional resources to fully understand my data privacy rights, as far as how that company or that service is handling things." P10 also later stated, "It's sort of the ultimatum, you either use the [mHealth] system or you don't. That's the only decision that you're allowed as a user…" Another participant, P09, shared a similar sentiment, "Do I really want to access this information, or do I want to have to go through a manual way or not do anything at all? Most of the time, I just accept it because I want to be able to pay my [medical] bill online or I want to be able to access MyChart [a personal health record] information online, and in order to do that, I have to accept it. So since you don't really get a choice and you need to get to it, you pretty much have to accept it anyway." These findings are consistent with research by (Utz et al., 2019) that notes the tensions users face when weighing tradeoffs between being informed and giving consent when interacting with privacy policies more broadly. Yet, participants discuss that when in these situations they feel they have limited autonomy especially if it is necessary or critical for them to use a mHealth system.

When manufacturers require consent without ensuring that users are sufficiently informed, or when not having access to a device or service is the only alternative option to consent, users shared that they begin to experience feelings that perpetuate transactional compliance as more important than costumer feelings or expectations. For example, P01 stated, "I think it's [providing privacy notices] strictly for compliance's sake. I don't know how many people actually read the privacy notices. So I hesitate to say it protects the consumer. I mean, it should protect consumers. It should protect both parties, quite frankly, but I just don't see that actually happening. I mean, I can't imagine, or I have to imagine the percentage of people that actually read terms of service or privacy notices or anything along those lines is remarkably small." As a result, participants believed that their interests are secondary to a manufacturer's compliance requirement, and they therefore experienced mistrust. We discovered that this mistrust is tied to the institutional systems and processes that govern mHealth applications. Although participant's degree of trust was inconclusive, some participants shared that it was attributed to unclear pre-market processes and the manufacturer or governing institution's history as it relates to quality. For example, P06 stated, "if I had a suspicion…my default is that makers have been vetted through the app store and they are trustworthy. But if I felt like there was something about their quality or trustworthiness that [there were] some sort of red flag, I might go into the privacy agreements. To be honest, if it was made… [by someone] that usually doesn't have our best interests in mind…that would motivate me to look [at] trust and quality." The limited choices related to consent and transparency of institutional practices, led participants to feel they had less autonomy in their privacy decisions related to mHealth applications.

4.2 Social Influences on Privacy Perceptions Influence Decisions

We learned that the perceptions of society or others also sometimes influenced participants' privacy decisions. Akin to the influence of social norms in TPB, we found that

participants sometimes see imbalances between technological advances and personal privacy on a macro socio-technical level. Some participants feared that society values the speed and convenience of mHealth technologies more than understanding their privacy implications. For example, P01 stated, "[the] balance of convenience and technology is one that's a very difficult one for me that I kind of struggle with just because I know how much you are giving up in the sense of privacy… I like to be more informed where that balance is with every individual device or piece of software, or whatever it is that I am interacting with… I like to be informed on how much of my life I am giving away or my information or my private data, or we will see how much of my soul I am selling to save eight minutes or to gain some form of convenience… I don't think that there is enough concern in the general populace for the level of information that is being collected about every individual…" Some participants therefore held a belief true privacy is hopelessly implausible due to the advancing tech market, which is consistent with attitudes of fatalism (Joo et al., (2021)). For example, P01 stated, "Unfortunately, privacy is a pipe dream that most people have given up." suggesting that they feel most users do not have autonomy in privacy decisions whether they like it or not. However, there were other users that were hopeful that future mHealth privacy research will consider these social concerns and influences and their implications.

Participants explained their privacy decisions are sometimes negatively affected by the type of health condition their mHealth device supports. Participants mentioned that mental health and addiction heighten their privacy decisions because these conditions have potential social stigmas and insurance implications. One participant was concerned about billing insurance for mental health issues. For example, P05 stated, "…when I worked in a health setting, you see a lot of patients coming in for mental health reasons or addiction reasons, and they didn't want their insurance billed, or they didn't want it to go through certain channels because they wanted to keep it highly private." Another participant was concerned about their employer receiving sensitive information about their addiction. For example, P08 stated, "…so say I had a drug problem or something, and there was an app for what I'm trying to handle that or something, I wouldn't want the fact that I was a drug addict being shared with an employer or anyone really. So, those kinds of things that could be looked on negatively…" As stated by these participants, social stigmas around sensitive health conditions have a role to play in their privacy decisions and also could impact their sense of autonomy leading to the decision not to engage with a mHealth application.

Participants also described a need for alternative modes of privacy discourse outside of traditional manufacturer notices that are typically provided. To address this, participants shared that they sometimes leverage social networks to communicate about critical mHealth privacy issues. One participant, P14 stated, "I think most people would learn through media or social media quicker than probably that a business would be notifying you that your data was compromised". Thus, participants expressed that their participation in social communication channels are needed for timely information that may affect their privacy decisions. So, participants expressed sometimes experiencing collective privacy influence. This collective influence could lead to developing apathy about privacy decisions due to perceived societal norms, more stringent views due to

fear of societal stigma, or alternative paths to build confidence in their decisions through social networks affecting their autonomy when engaging with mHealth applications.

4.3 Contextual Nascence: Navigating Black Box Interoperability and Historical Preconceptions

We learned that participants' interactions with privacy notices vary significantly but may originate from unique historical preconceptions, such as black box interoperability and the evolution of health and technology. For example, interoperable mHealth environments collect and process various forms of sensor and self-reported personal health data. This data is often embedded in artificial intelligence (AI) or other personalized systems whose architecture enables health management solutions similar to those described in other work (Danaher et al., 2015). While these architectures are innovative, participants expressed privacy concerns about technologies such as proactive AI systems that continually collect their data and push untraceable targeted-marketing material. This raises broader questions about the role of emerging technologies such as IoT or voice technologies in shaping users perceptions of mHealth technologies and users interactions with health applications provided by those devices. For example, P09 stated, "…Siri and the Amazon Echo are listening all the time [and] can get information and they're going to hear private health information. If, you know, somebody's listening or they're going back and reviewing vital recordings, as they're supposedly trying to make Siri better and more interactive with better programming. There are people who hear that private information. So because it's recorded near your house, private information could also be out there if that's what happens, what was recorded at that point in time." Participants were generally uncertain about the AI black box (Lau et al., 2018), but were tangibly concerned about the inability to trace data effectively across its lifecycle, and especially when it is shared or sold for other purposes. For example, P10 stated, "…this kind of goes along the lines of sharing or understanding how my data is being shared with other companies or the service provider I am doing business with…If I start to get targeted or oddly specific targeted ads that seem to be coming from my interactions with one system in particular, that could prompt me to take a look and maybe try to get a better understanding of just how much data is being collected and how it's being used. And just kind of trying to connect the dots if I get very targeted marketing on different devices and I can try to trace it back to a certain application…".

Participants also perceived healthcare's historical evolution as a motivational factor towards privacy. Health technologies such as mHealth are burdened with negative historical connotations for various reasons such as public cases of individuals' health data rights being violated. Participants explained that the rapid prevalence of notices for various technologies is one reason why some pre-mHealth generations have negative views about mHealth technologies. For example, P07 stated, "I think at this point, I'm young enough to expect them [privacy policies] to be there and old enough to remember when they weren't." Another negative historical connotation was explained by P02, who stated, "the older cases of like Henrietta Lacks, they used her [information] and she never knew." We found that these historical references and events influenced how participants perceived privacy in certain social groups.

In summary, we learned that subjective norms around interoperable environments (e.g., wearables and remote patient monitoring) in the health context, social influences, and changing motivations each influence participants' privacy interactions, which ultimately affects their perception of autonomy and trust in those interactions. By uncovering these subjective norms, we identified unique relationships with trust that may not have been clearly articulated previously in the mHealth design space.

5 Discussion

Through the lens of TPB, our research finds that mHealth users are unengaged with privacy policies and feel there is a chasm between their individual needs and the controls provided by the privacy community. Overall, our research suggests that mHealth users generally agree that privacy policies are beneficial and crucial for mHealth applications; however, they encounter persistent challenges when engaging with those policies. Specifically, we found that not sufficiently characterizing user' perceptions of internal and external motivations may obfuscate real opportunities for making privacy language more engaging and bridging the gap to help users understand essential information. As such, one result may be that end-users do not understand how the design of these privacy solutions are intended to protect them. Thus, having superficial awareness without knowledgeable engagement does not actually support autonomy and trust in mHealth applications. Our research builds on existing literature [Cunha et al., (2020), Leon et al., (2015), Vilaza et al., (2019), Gupta, (2018)) by advocating for the development of privacy solutions to be behaviorally and contextually orientated in order to uncover real user facing problems when interacting with mHealth privacy policies. Improving users' ability to understand language and recognize dynamic mHealth privacy environments relies on systematically assessing motivational intentions that engage users beyond basic privacy awareness. Further, we found that perceived control over one's mHealth privacy is unrealized partly in fact due to the inability to tangibly see, interact, and understand what privacy means when engaging with a mHealth technology. Thus, many users feel they lack autonomy when engaging with mHealth privacy policies, but due to the criticality of the context - managing health, users feel compelled to comply or completely disengage despite their concerns. Our results show that designing for motivationally charged engagement and understanding by leveraging social factors may be one effective way to optimize autonomy-support and trust in mHealth solutions. We discuss these implications in the following sections.

5.1 More Control Does Not Equal More Autonomy

Our work considers perceived autonomy through the lens of Self Determination Theory (Deci et al., 2012), where autonomy is having the choice and will to act according to personal goals and values. For health-related technology design, (Calvo et al., 2020) distinguishes autonomy from independence and control, noting that perceived autonomy can also be influenced by individual behaviors, lifestyle or society, which in-turn impacts adoption. Significant work has been done to simplify the experience that users have with privacy policies (Acquisti et al., 2017) and provide them with more control over their

data, consent, and nudging interactions (Cunha et al., (2020), Degeling et al., (2018), Schaub et al., (2017), Utz et al. (2019)). Yet, due to some of the historically untrustworthy actions that occurred that sit at the intersection of health and privacy (Grossmann et al., 2011), some users still are wary, influencing their perceptions of mHealth technologies. To address questionable trust and adoption in mHealth systems that collect and process health data, researchers and industry practitioners have seemingly held the position that providing more ways for users to access and manage personal data is a sufficient baseline for control (Schaub et al., (2017), (Atienza et al., 2015)). However, we uncovered that users' perceptions and expectations of privacy control often do not equate to the independence that is needed for autonomy. Therefore, based on our data we conclude that there is a conflated belief that control is the same as autonomy. In the design of health and well-being technologies, often autonomy extends beyond the binary concepts of control and is defined as a users' feeling of agency or their ability to act based on their goals and values (Peters et al., 2018). In the context of mHealth privacy, while it is reasonable to assume that personal responsibility is essential for consenting and using mHealth technologies, non-privacy-neutral perceptions inherently exist when users are tasked with deciding to use a service or not (binary opt-in vs. opt-out). This is further compounded by the fact that notice-choice structures present content that are likely not to be read in the first place (Meier et al., 2020). When agreements are in place with conditions that are non-negotiable to the user's existing motives or beliefs, this creates questions of perceived control over one's privacy and whether the application actually supports users' autonomy, and is deserving of trust.

Our findings highlight users' beliefs that there are not enough alternative ways of getting people to engage with their mHealth data privacy practices, specifically informed consent interactions. Further, offloading all the privacy decisions at the launch of a new app is not only contradicting the benefit of the mHealth app, but it also ignores the dynamic ways that people choose to be informed and interact with their sensitive information. In the future, it would be beneficial for usable privacy researchers and industry professionals to explore alternative strategies that focus on personalized and emotional engagements with mHealth data privacy in order to support autonomy, while also distinguishing this work from traditional views about privacy control that often focuses on actions. In similar discussions, (Christman, 2020) distinguishes basic and ideal autonomy where basic autonomy implies that users are free from influence and imply they are not under constricting conditions. We also posit that patients with health conditions who seek support from mHealth technologies are inherently constricted in autonomy and thus are forced to weigh utility-tradeoffs unfairly. While this context of autonomy relates to other work regarding "contextual integrity" (Wijesekera et al., (2015), Zimmer, (2018)), we find that meeting user expectations is not simply about control (e.g., permissions, etc.), but also recognizing the role of changing awareness and mental processing, particularly on the side of social and historical influences. Our research extends prior work that examines contextual factors related to general privacy policy design (Micinski et al., (2017), Votipka et al., (2018), Squicciarini et al., (2014)), but we extrapolate factors unique to supporting autonomy with mHealth's privacy interactions.

5.2 Balancing Perceptions of mHealth Privacy Autonomy and Automation

Privacy autonomy, through the lens of independent engagement and trust, is inherently challenged because of limited support and choices (Cunha et al., (2020), Schaub et al., (2017)). However, our examination of users' self-reported behaviors indicates that understanding mHealth privacy language is also a barrier to fully engaging with a technology. We extend the need to decouple the domains of being informed and intentional consent in order to focus research towards understanding language over simply improving consent interactions. Making information comprehensible for users reach educational and governance systems because both are needed to scale health and consumer applications, especially when data collection is essential in the user's health journey. In some mHealth technologies, such as the wearable Apple Watch, users are able to select the data that may be collected about them (i.e., biometric identifiers) conditional to the practices that are employed in a given app's functionality. Using gamification techniques may be another considerable way of building user knowledge about the personal data collected about them, which is supported in the research by (Simon et al., 2021) that describes cognitive absorption for privacy decision-making because of engaging gamification. Other research (Mavroeidi et al., 2020) also considers using gamification for engaging users about privacy. However, we also suggest that in the future, it could be useful to investigate the role of gamification in building value constructs aimed to incentivize (or motivate) learning and understanding complex mHealth data privacy.

Collective privacy influence is a unique area that emerged from our interviews because it highlights both the benefit and responsibility of understanding social contexts when developing policies about mHealth privacy. Although this finding is similar to users engaging in health-based communities for health support (Kordzadeh et al., (2017), Danaher et al., (2015)), it is unique in the sense of mHealth privacy because it exposes a gap where individuals and their social influences are not currently aligned, which affects these users' perceived privacy control, thus autonomy and trust. This is similarly discussed in research by (Gupta, 2018) that identifies external influences (e.g., such as prior experience) on older adults' general privacy behaviors, but the emerging theme from our interviews recognizes the social norms, highlighted in behavioral theories such as TPB (Icek, 1991), play a unique role in dynamic mHealth privacy behaviors. Various socially oriented topics arose from our data ranging from meta views on balancing social and personal privacy initiatives, situation avoidance for privacy discourse, data privacy footprint in social networks, balancing privacy advocacy and improving services, and providing community for individuals with stigmatized health conditions. While these topics range in variety and abstraction, they construct a basic model for the relationship between social influences and perceived individual privacy attitudes, thus extending work (Zou et al., (2020), Guo et al., (2016)) by detailing unique behavioral intentions used as a vehicle for trust in mHealth systems. It is for this reason that we suggest that future usable mHealth privacy research must continue to investigate these topics and explore opportunities to leverage and enhance these outside constructs for the development of truly autonomy-supporting privacy interactions.

Furthermore, potential design directions that strike a balance between autonomy and automation may need to focus primarily on consent, transparency, and trust. Specifically, designing preferences at the time when the user provides consent must be careful

in not overwhelming the intended users with options that seemingly appear outside of the perceived guardrails. This means that while some configurable parameters may be needed, having too many options can lead to confusion or make users feel like they are completely on their own in their privacy decisions. This nuanced position is contrast to the notion of having complete awareness and control as premised in previous research (Andrews, (2019), Schaub et al., (2017)), but it more importantly must match users expectations about broadly applied privacy preference modeling across mHealth apps. Moreover, consent modeling is inherently dynamic over time and between people who share information in mHealth app environments. For example, collaborative privacy sharing models (Petronio, 2010) take into account multiple parties, but how these collaborative agreements change with participant preferences over time present uncertainty, thus designing for clear user-roles and control are critically important. Lastly, fostering trust and transparency requires a transparency about black box environments where data are collected, processed, and stored. Such transparency-enhancing tools are acknowledged as helping promote privacy and trust (Janic, et al., (2013)), but an importantThis mechanism of for this visibility must ensure traceability of data usages and clear verifiable levels of control by the user over data in those specific environments.

5.3 Limitations

One limitation of our work is that our study is retrospective of behaviors and does not actually observe behaviors with privacy policies. While the self-reported accounts provided by participants provide insights into their experiences with mHealth privacy policies, additional studies of direct user behavior may uncover additional challenges and design implications. Our work is also qualitative which is useful for providing an in-depth understanding of users' attitudes and perceptions. However, one tradeoff of qualitative work is that findings are not generalizable (Leung, 2015). We provide a rich, thick description to aid transferability, but our work like other qualitative work (Joo et al., (2021), Martin-Hammond et al., (2019), Zhang et al., (2021)) is likely limited based on the context in which it was carried out. Further, as we collected data we began to see recurring ideas, and continued until we stopped seeing new data, which. This is consistent with the processes for analyzing qualitative data., however our While our sample is small and may be limited by certain participant demographics, such as some participants that were familiar with familiarity with privacy policies, we believe this to still be a valuable step in the direction to explore this research further and look to consider age-based and other demographic perspectives in future work and therefore some users' privacy concerns may not be represented in our findings. Our $N = 15$ is slightly higher than other qualitative interviews (Caine, 2016) conducted by HCI researchers, however, data reached saturation at 12 participants where we noticed consistent responses with fewer new points emerging. We completed an initial review of all transcripts excluding those without response variation to determine those to include in agreement calculations. We used (McDonald et al., 2019) for determining our agreement approach. Our analysis approach was consistent with their arguments against solely using IRR for agreement. These are considerations for future research.

6 Conclusion

In this paper, we used existing behavior models as a lens to understand users' privacy experiences, behaviors, and perspectives toward mHealth data privacy policies. From 15 semi-structured interviews with adult users of mHealth applications, we extend knowledge of users' experiences and unmet needs for privacy policy design that influence users' behaviors toward mHealth applications. Through the lens of the Theory of Planned Behavior and SDT, we characterize factors beyond personal data control and consent that influence users' sense of autonomy when engaging with mHealth privacy policies. Finally, we provide unique considerations for privacy policy design that focus on improving consent preferences, transparency of privacy control statuses, and building trust on a multiple levels.

Acknowledgments. Special thanks to the participants that shared their experiences and Davide Bolchini, Ph.D., for assisting with editing.

Appendix

Table 1. Participant Demographics

P#	Gender	Age	Highest education level	OS	mHealth app usage	Privacy notice frequency
1	Male	43	Graduate degree	iOS	Daily	Weekly
2	Female	31	Graduate degree	AOS	Daily	Daily
3	Male	47	Graduate degree	iOS	Monthly	Monthly
4	Male	31	Graduate degree	iOS	Daily	Weekly
5	Female	39	Undergraduate degree	iOS	Daily	Annually
6	Male	49	Graduate degree	iOS	Monthly	Monthly
7	Female	39	Some college	iOS	Daily	Weekly
8	Female	67	Undergraduate degree	iOS	Daily	Monthly
9	Female	56	Doctorate degree	iOS	Daily	Daily
10	Male	28	Undergraduate degree	iOS	Weekly	Monthly
11	Female	57	Graduate degree	iOS	Daily	Weekly
12	Male	37	Some college	iOS	Weekly	Weekly
13	Female	32	Undergraduate degree	AOS	Daily	Weekly
14	Male	28	Undergraduate degree	iOS	Weekly	Monthly
15	Male	59	Some college	iOS	Daily	Weekly

Table 2. Preliminary Themes

Question	Answer	Theme
Meaning of "data"	Collected	Informational inputs and outputs
	Interpreted	
	Analyzed	
	Processed	
	Decision derivation	
Meaning of "privacy"	Confidentiality	Limiting exposures
	Access	
	Hopelessly implausible	Socio-technical influences
	Personal protection	Personal interventions
	Control	

Table 3. Study interview mobile health privacy policy probes (stimuli)

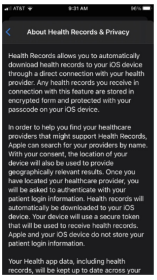
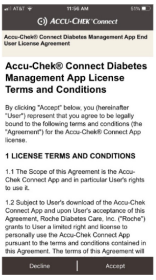
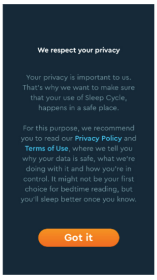
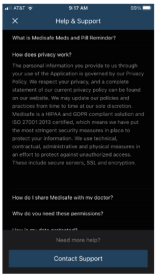
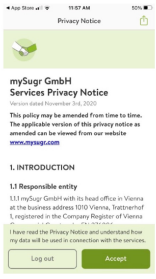
Apple (General)	Accu-Chek Connect (Diabetes)	Sleep Cycle (Sleep)	Medisafe (Medications)	mySugr (Diabetes)
				

Table 4. Methodological process

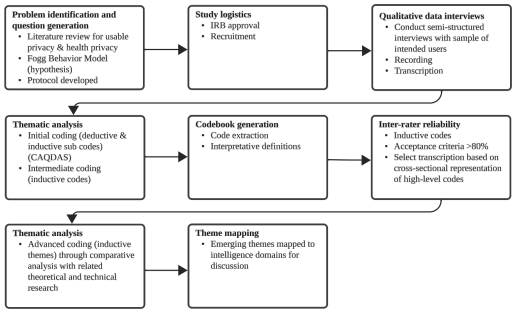


Table 5. Initial & Intermediate Thematic Codes

Emerging Themes	Privacy Challenges (Codes)
Disconnected cognition for assessing value	Modern data privacy interpretations
	Knowledge, emotional, and identity benefits
	Disconnected knowledge to propose value in pervasive environments
Challenged agency - limited freedom of choice	Incongruent consent
	Insufficient options
	Information retrieval
	Inflexible and disabled solutions
	Multivariate burdens and utilities
	Unclear privacy requirements for players
	Privacy requirements for preventing harm to organization and user
Customizable, trustworthy, and engaging solutions to build sensational experiences	UX/UI for improving privacy engagement
	Privacy volume and comprehension affecting app authenticity and trust
	Custom feature development that enable privacy interactions
Privacy awareness anticipations for the future	Balance between social and personal privacy paradigm
	Privacy competence to ensure end user interests are core

(*continued*)

Table 5. (*continued*)

Emerging Themes	Privacy Challenges (Codes)
	Awareness about where data exists in the wild and corrective steps to reduce its footprint
External influencers	Avoiding situations where privacy beliefs are challenged
	Knowing data footprint in connected social networks
	Balance user privacy advocacy and improving services
	Community for those with stigmatized health conditions
Unique Motivators	Mapping app's utility to types of required privacy interactions
	UX/UI not designed for diverse intended users' needs
	Robust and quality-driven app vetting to produce trust
	Privacy information designed for simple, personalized risks/controls
	Data types with high motivation
Supporting contextual autonomy through accessibility	Visual limitations persist and inhibit ability pursuant modality
	Ability dependent on environment
	Discern problem solving (self-diagnosis and resolution) VS. Seeking professional consultation
	Attention limitation
	Efficient, simple, and gratifying enable ability
Triggering autonomy through automation	Early declaration of an app intended use and relationship to your data
	Undesirable early interactions impacting attention and experience
	High frequency notices inducing questions and fatigue
	Overcoming negative historical connotations

(*continued*)

Table 5. (*continued*)

Emerging Themes	Privacy Challenges (Codes)
	Unclear time-value tradeoff
	Enable automatic prompts for reduced manual/mental comparisons
	App launch and preset schedule for data change notification
	Interaction and illustration for privacy change engagement
	Social risk-reward engagement
	Uncertainty in AI

References

Acquisti, A., et al.: Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput. Surv. 50(3): Article 44 (2017)

Al Ameen, M., Liu, J., Kwak, K.: Security and privacy issues in wireless sensor networks for healthcare applications. J. Med. Syst. **36**, 93–101 (2012). https://doi.org/10.1007/s10916-010-9449-4

Andrews, V.: Analyzing awareness on data privacy. In: Proceedings of the 2019 ACM Southeast Conference, pp. 198–201. Association for Computing Machinery, Kennesaw (2019)

Arora, S., Yttri, J., Nilse, W.: Privacy and Security in Mobile Health (mHealth) Research. Alcohol Res. Current Rev. **36**(1), 143–151 (2014)

Atienza, A.A., et al.: Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. J. Health Commun. **20**(6), 673–679 (2015). https://doi.org/10.1080/10810730.2015.1018560

Bartoletti, I.: AI in Healthcare: Ethical and Privacy Challenges. Springer International Publishing, Cham (2019)

Bertino, E., et al.: Internet of Things (IoT): Smart and Secure Service Delivery. ACM Trans. Internet Technol. **16**(4): Article 22 (2016)

Caine, K.: Local standards for sample size at CHI. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 981–992, May 2016

Calvo, R.A., Peters, D., Vold, K., Ryan, R.M.: Supporting human autonomy in AI systems: a framework for ethical enquiry. In: Burr, C., Floridi, L. (eds) Ethics of Digital Well-Being. Philosophical Studies Series, vol. 140. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50585-1_2

Cameron, J.D., Ramaprasad, A., Syn, T.: An ontology of and roadmap for mHealth research. Int. J. Med. Informatics **100**, 16–25 (2017). https://doi.org/10.1016/j.ijmedinf.2017.01.007

Chen, Y., et al.: Privacy games. ACM Trans. Econ. Comput. **8**(2), Article 9 (2020)

Christman, J.: Autonomy in Moral and Political Philosophy. The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/

Chun Tie, Y., Birks, M., Francis, K.: Grounded theory research: a design framework for novice researchers. SAGE Open Med. **7**, 2050312118822927 (2019). https://doi.org/10.1177/2050312118822927

Cunha, J.A.O.G.d., Aguiar, Y.P.C.: Reflections on the role of nudges in human-computer interaction for behavior change: software designers as choice architects. In: Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems. Diamantina, Brazil, Association for Computing Machinery: Article 56 (2020)

Danaher, B.G., et al.: From black box to toolbox: outlining device functionality, engagement activities, and the pervasive information architecture of mHealth interventions. Internet Interv. **2**(1), 91–101 (2015)

Deci, E.L., Ryan, R.M.: Self-determination theory. In: Van Lange, P.A.M., Kruglanski, A.W., Higgins, E.T. (eds.) Handbook of Theories of Social Psychology, pp. 416–436. Sage Publications Ltd. https://doi.org/10.4135/9781446249215.n21

Degeling, M., et al.: We value your privacy … now take some cookies: measuring the GDPR's impact on web privacy. Informatik Spektrum **42**(5), 345–346 (2018)

Detweiler, C.A., Hindriks, K.V.: A survey of values, technologies and contexts in pervasive healthcare. Pervasive Mob. Comput. **27**, 1–13 (2016)

Peters, D., Calvo, R.A., Ryan, R.M.: Designing for motivation, engagement and wellbeing in digital experience. Front. Psychol. **9** (2018). https://doi.org/10.3389/fpsyg.2018.00797

Schomakers, E., Lidynia, C., Ziefle, M.: Listen to my heart? how privacy concerns shape users' acceptance of e-health technologies. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 306–311 (2019). https://doi.org/10.1109/WiMOB.2019.8923448

Ferreira, A., et al.: Perceptions of Security and Privacy in mHealth. In: HCI for Cybersecurity, Privacy and Trust, Cham, Springer International Publishing (2021)

Fishbein, M.: A theory of reasoned action: Some applications and implications. Nebr. Symp. Motiv. **27**, 65–116 (1979)

Floridi, L., Cowls, J., Beltrametti, M., et al.: AI4People—an ethical framework for a good ai society: opportunities, risks, principles, and recommendations. Mind. Mach. **28**, 689–707 (2018). https://doi.org/10.1007/s11023-018-9482-5

Fogg, B.J.: A behavior model for persuasive design. In: Proceedings of the 4th international Conference on Persuasive Technology, pp. 1–7, April 2009

Guo, X., et al.: The privacy–personalization paradox in mHealth services acceptance of different age groups. Electron. Commer. Res. Appl. **16**, 55–65 (2016)

Gupta, B., Chennamaneni, A.: Understanding online privacy protection behavior of the older adults: an empirical investigation. J. Inf. Technol. Manag. **29**, 1–13 (2018)

Hutchinson, H., et al.: Technology probes: inspiring design for and with families. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Ft. Lauderdale, Florida, USA, Association for Computing Machinery, pp. 17–24 (2003)

Poyner, I.K., Sherratt,R.S. : Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2018, pp. 1–5 (2018). Doi: https://doi.org/10.1049/cp.2018.0043

Icek, A.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)

Institute of Medicine (US) Roundtable on Value & Science-Driven Health Care. Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary. Washington (DC): National Academies Press (US); 2010. 5, Healthcare Data as a Public Good: Privacy and Security. https://www.ncbi.nlm.nih.gov/books/NBK54293/

Institute of Medicine (US); Grossmann C, Powers B, McGinnis JM, editors. Digital Infrastructure for the Learning Health System: The Foundation for Continuous Improvement in Health and Health Care: Workshop Series Summary. Washington (DC): National Academies Press (US); 2011. 8, Fostering the Global Dimension of the Health Data Trust. https://www.ncbi.nlm.nih.gov/books/NBK83578/

Iwaya, L.H., Babar, M.A., Rashid, A.: Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organisational Culture, and Current Practices (2022). arXiv preprint arXiv: 2211.08916

Joo, E., Kononova, A., Kanthawala, S., Peng, W., Cotton, S: Smartphone Users' Persuasion Knowledge in the Context of Consumer mHealth Apps: Qualitative Study. JMIR Mhealth Uhealth **9**(4), e16518 (2021). https://mhealth.jmir.org/2021/4/e16518, https://doi.org/10.2196/16518

Kolovson, S., et al.: Understanding participant needs for engagement and attitudes towards passive sensing in remote digital health studies. In: Proceedings of the 14th EAI International Conference on Pervasive Computing Technologies for Healthcare, Association for Computing Machinery, pp. 347–362 (2020)

Kordzadeh, N., Warren, J.: Communicating personal health information in virtual health communities: an integration of privacy calculus model and affective commitment. J. Assoc. Inf. Syst. **18**, 45–81 (2017)

Nurgalieva, L., O'Callaghan, D., Doherty, G.: Security and privacy of mHealth applications: a scoping review. IEEE Access **8**, 104247–104268 (2020). https://doi.org/10.1109/ACCESS.2020.2999934

Lau, J., et al.: Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In: Proc. ACM Hum.-Comput. Interact. 2(CSCW): Article 102 (2018)

Leon, P., et al.: Privacy and behavioral advertising: towards meeting users' preferences. In: PPS '15: Second SOUPS Workshop on Privacy Personas (2015)

Janic, M., Wijbenga, J.P., Veugen, T.: Transparency enhancing tools (TETs): an overview. In: 2013 Third Workshop on Socio-Technical Aspects in Security and Trust, pp. 18–25. IEEE, June 2013