Research Summary

Privacy with Smart Home Devices [Lau et al., Zeng et al., Taubassum et al.]

When it comes to smart home devices, concerns with data collection could be mitigated depending on how much the user trusted the manufacturer of the device (Lau et al., Zeng et al., Taubassum et al.). A common attitude that user's reported was that they had "nothing to hide" and thus no one would bother to target them specifically (Lau et al., Taubassum et al.) . User's also reported that they felt that there was a tradeoff between privacy and convenience. In some studies, participants "explicitly identified a tradeoff, requiring that one accepts security or privacy risks in exchange for the functionality and convenience of a smart home (Zeng et al., Taubassum et al.). Participants reported being aware that the data was being collected for targeted ads, but felt uncomfortable with the idea that their voice commands would be used for that purpose (Lau et al). In the same study non-users of smart home devices reported choosing not to use smart home devices either because they did not find them useful or did not trust the manufacturer of the smart home device (Lau et al). In addition, they found that all participants expressed privacy concerns with third parties. Nonusers did not trust companies to keep data to themselves while users trusted companies to not share the information. Interestingly, while both users and non users of smart home devices generally found targeted ads to be "creepy", they were preferable to irrelevant ads because they found them to be useful (Lau et al). User's privacy concerns were also "largely shaped by their own experiences in other computing contexts and with organizations' " (Taubassum et al.). Another reason why users did not seem to be concerned was because they viewed marginal risk to be minimal, meaning that because so much information has already been collected or is available, the smart home device would not increase their privacy risk (Taubassum et al.). Another concern that was identified was that if there are multiple users of a smart home device, the administrator can use it to spy on the other users (Lau et al.). Users also expressed concerns with physical security, such as others being able to access the locks or being able to know when the users are home. They noted that they were less concerned with data breaches of their phone or laptop because they can remotely wipe it.

Privacy and online data collection [Kang et al., Phelan et al., Zhao et al.]

Participants reported trust as a factor in their privacy concern because participants felt that they could trust the creator's intentions and that the application truthfully described exactly what it did (Phelan et al.). Some factors that played into trust were knowledge that other people used the same service, reputable brand, terms of service, certificates, warnings, and whether or not they had a bad experience on the site (Kang et al.). One study sought to understand people's mental models of the internet and found that technical background did not influence participants' actions towards protecting their privacy, but the mental models that the participants provided were indicative of the number of threats that they perceived (Kang et al.). In the same study, participants reported not taking protective measures because doing so would sacrifice effectiveness or convenience (Kang et al.). Other reasons included poor usability of privacy tools or software and feeling of helplessness and lack of procedural knowledge (Kang et al.).

Another study sought to understand the privacy paradox as it pertains to online privacy concerns (Phelan et al.). They reason that this paradox can be explained by two concepts – intuitive concern and considered concern. Intuitive concern relates to a user's "gut feeling" about a particular situation, while considered concern refers to the user's rational judgement (Phelan et al.). In other words, whether the data collection practice was "creepy" and whether they were "bothered" by it. Generally, whether the intrusion was bothersome was the most important and the intrusion's creepiness was largely dismissed. For instance, some participants reported that they felt that targeted advertisements were "weird", but weren't necessarily bothered by it. Trust played a big role in lowering both intuitive and considered concern and marginal risk only played a role in lowering considered concern and gave users a justification for ignoring intuitive concern. Participants generally reported feeling uncomfortable when they felt that they were "being watched" by data collectors. This was usually described by an experience where they became aware of a data collector's presence, for instance through targeted advertising, but did not feel that they were being watched constantly. Another study tried to understand children's perceptions of privacy risks online. They found that children missed the risks of personalized game promotions, cautious of pop ups that ask for personal information, and cautious of tracking behavior of apps (Zhao et al.).

Privacy and Other HCI [Lee et al., Hamidi et al., Wilkowska and Ziefle]

Researchers have also studied privacy in the context of human-robot interaction. In this study, researchers interviewed participants on their attitudes towards Snackbot, a social workplace robot. All the participants said that they would not be concerned about being recorded as long as they were informed and aware that the robot was recording. Half of the participants noted that they would be more comfortable with accidental recordings if they were notified of such a possibility. However, they also noted that since this robot was in the workplace, they would not be engaging in behavior that they shouldn't be doing anyways. Other participants expressed concern over the potential misuse of accidentally recorded videos. Regardless, all participants wanted to be notified whether they were accidentally recorded by the robot (Lee et al.). Researchers have also studied privacy in the context of adaptive assistive technologies. Most privacy concerns related to how data could be used without explicit consent. Some were concerned that the data was not going to be used as promised by the application. However, some noted that this feeling of helplessness was mitigated if they paid for the application (Hamidi et al.). Privacy has also been studied in the context of e-health technology. People with good health conditions preferred a relatively high degree of discreteness, anonymity, and intimacy and did not want their e-health technology usage to be visible to others, while those with poorer health paid less attention to privacy. The study noted that it is "understandable too, that sickly persons are rather willing to make their course of disease or … vital parameters transparent and easily accessible, in order to facilitate the work of healthcare professionals" (Wilkowska and Ziefle).

Privacy Summary (Similarities and Differences)

In studies on online data collection and smart devices, both studies showed that users' trust was a major factor in privacy concerns. In all three types of studies mentioned, participants addressed trust in how the companies will use the data being collected. Participants in both contexts expressed that they had a negative opinion of targeted ads, with them being described as “creepy”, “weird”, or “annoying”. In contrast, participants in the smart home studies preferred targeted ads over irrelevant ads. Participants in studies related to online data collection reported feeling that they felt “being watched” when they saw a targeted ad, but that feeling soon went away. Participants who used certain products expressed being able to trust the companies to not share their data. Participants also viewed privacy and convenience as a tradeoff in the context of smart home devices and online data collection. This was also implied in the e-health technology study, where they found that patients with poorer health cared less about privacy, presumably because making their health data accessible will help facilitate the work of health care professionals. Another similarity between these types of studies was that lower marginal risk played a role in making participants less concerned about privacy. In online data collection and adaptive assistive technologies, participants reported feeling helpless when it comes to protecting their privacy. Interestingly, some participants mentioned that the feeling of helplessness was mitigated if they paid for the application. It also seems that users feel more comfortable if there is some degree of transparency in the data collection practices. For instance, users of adaptive assistive technologies were concerned about their data being used without their consent. Participants in one smart home devices study felt uncomfortable with their data being shared with third parties, with one nonuser reporting that if their data was shared with third parties, they would not know how that data was being used. In addition, participants in the HRI study reported that they would be fine with being recorded by the robot as long as they knew that they were being recorded. Even with the study on children’s perceptions of privacy, tracking behavior was unfamiliar to them, so they felt that it was best to stop using the app and tried to find out more information on how the data was going to be used. A concern that was raised in a smart home devices study that was not present in other studies was that users were uncomfortable with the idea of using voice recordings for targeted advertising.

Chatbots and Self-disclosure [Lee et al., Lee et al.]

Chatbots have shown great potential in mental health treatment to promote self-disclosure. In one study, researchers sought to understand the effect of chatbot self-disclosure on participants’ self disclosure. There were three groups of participants, one where the chatbot did not disclose at all, one where the chatbot disclosed some information, and one where the chatbot disclosed deeply. They found that there was more disclosure from the participants when the chatbot discloses more. Some participants in the group with deep chatbot self-disclosure also noted that they felt responsible to answer questions in detail since they felt that they were “genuinely exchanging information” with it. Many participants noted that they felt comfortable disclosing to the chatbot because they did not have to worry about the judgment of the conversational partner. In another study, the chatbot was treated as a mediator between a mental health professional and patient; researchers sought to understand how using a chatbot as a mediator affects self-disclosure to a real mental health professional. In the study, the participants were split up into the same three groups as mentioned before. Then, after chatting with the bot, they were asked to share their conversations with the chatbot with a real mental health professional, while in the other groups, it was about trust in the research team behind the chatbot to deal with their information properly. They found that the group with deep self-disclosure from the chatbot trusted the chatbot, which spilled over to trust in the mental health professional. The study concluded that “the findings imply that the chatbot that offered deep disclosure had the potential of serving as an effective mediator to facilitate the people’s self-disclosure of sensitive information. Interestingly, trust in the chatbot did not increase over time within any of the groups in both studies. While both studies briefly touched on potential privacy issues (i.e. the risk of over sharing private information), they only discuss potential design solutions to mediate this (a feature to allow them to edit their response).They did not discuss the tradeoff between the personalization of the conversation and the user’s privacy and how that may affect the user’s experience with that chatbot.

Creepiness and HCI [Yip et al., Torkamaan et al.]

In another study, researchers sought to understand children’s perceptions of creepy technologies. They found that children feared physical harm by technology. In addition, they feared that the technology would stalk their families and cause a loss of attachment with their family. However, the children did not mind the idea of their parents using technology to surveil them as long as they knew information was being sent to their parents. Children also expressed being uncomfortable with the idea of technology mimicking their humans and animals and those with an ominous physical presence (looks, sounds, and feels) (Yip et al.). Researchers also tried to understand the factors that affect the creepiness of recommendations. They found that recommendations for products or services related to a sensitive topic (products for a different age group, mental health) can make them uncomfortable or annoyed. They also found that recommendations that match the user’s preferences perfectly can be creepy, but if the users are not able to explain why they received a recommendation, that could also be viewed as creepy. Other users also reported feeling creeped out if a recommendation is based on a forgotten user history, limited past interaction, or an already fulfilled need. (Torkamaan et al.).

Person-person creepiness

Research in creepiness is fairly new and is broadly defined. The definition of creepy situation given in one of the papers is a situation that “elicits uneasy feelings and involves ambiguity” (Langer and König). In the same paper, researchers have tried to create a scale called CRoSS which measures perceived creepiness of a situation. When testing the validity of the scale, they found that creepiness is positively correlated to privacy concerns, positively correlated to computer anxiety, negatively correlated to transparency, and negatively correlated to controllability of the situation. When further testing the validity of the study, they found that women will report more creepiness than men and the experimental situation during the night will evoke more creepiness than during the day (Langer and König). In a more well known study, researchers sought to understand the “building blocks of creepiness”. At a high level, what the researchers found was that the perception of creepiness is a response to the ambiguity of threat. Individuals who display unusual patterns of nonverbal behavior (someone standing too close), odd emotional responses (someone laughed at unpredictable times), or highly distinctive physical characteristics (someone has a peculiar smile) are outside of the norm, and by definition unpredictable (McAndrew and Koehnke). They also found that males are more likely to be perceived as creepy. Interestingly, this is in contradiction to the first paper, which found that a female experimenter will evoke more creepiness than a male experimenter. In another study, researchers sought to understand how judgments of creepiness are made, mostly focusing on the aspects of the appearance of the person that makes someone creepy. They also addressed that discussions around creepiness usually revolved around behaviors that are socially unacceptable (Watt and Maitland).

Person-Person Interaction Impressions [Szczurek et al., Leander et al., Weisbuch et al.]

Other studies on person to person interactions were not explicitly related to creepiness, but are still loosely related to creepiness. For instance, one study sought to understand people's impressions of social deviants, which for this study are people who express counter-normative opinions or possess a stigmatized identity. The researchers showed the participants a video of someone reacting to an image and asked the participants what they thought of the person in the video. In general, the researchers found that participants viewed those who had congruent responses (i.e. smiling at happy pictures) were viewed more positively than those who had deviant responses (i.e. smiling at gruesome pictures) (Szczurek et al.). In another study, researchers sought to understand how behavior mimicry influences feelings of coldness. They found that people literally feel colder in response to inappropriate amounts of behavioral mimicry depending on the interaction style of the interaction partner (affiliative vs task oriented interaction), individual differences (socially interdependent vs socially independent), and racial differences. They found that participants felt colder with an affiliative experimenter if not mimicked and colder with an task-oriented experimenter if mimicked. They also found that interdependent participants who were not mimicked felt colder and independent participants who were mimicked felt colder. Lastly, they found that those engaging in cross race relations felt colder (Leander et al.). In another study, researchers wanted to understand how verbal-nonverbal consistency affects first impressions (i.e. facial expression vs vocal behavior). Overall, the researchers found that inconsistency between nonverbal and verbal affect resulted in a negative impression. They also found that people who exhibited more positive affect were more likeable than those who exhibited less positive affect, but the relationship with likeability was stronger for nonverbal affective expressions than verbal affective expressions (Weisbuch et al.).

Creepiness Summary

Creepy situations described in these studies seem to relate to uncertainty. For instance, Siri talking out of nowhere could be thought of as an uncertain situation because there is no explanation for why Siri would talk unprompted, inconsistent behavior (i.e. inconsistent facial expressions and vocal behavior), or odd emotional responses (i.e. laughing at random times), were viewed negatively. A lot of the creepiness studies also was related to physical appearance, such as describing physical features that would make someone seem creepy. In general, those who displayed deviant social behavior (standing too close, smiling at gruesome pictures), were viewed negatively. Technology that was human-like was also perceived as creepy.

Privacy and Creepiness (Overlap between Privacy and Creepiness, Similarities, Differences)

Most of the privacy and creepiness intersection was related to targeted advertising. One book talks about privacy and creepiness in the context of targeted advertising. They note that marketers should not create messages that are out of context to avoid coming off as creepy. Other suggestions include, engaging in trustworthy behavior (transparency, establishing a relationship with customers and engaging with them on a human level) and maintaining contextual integrity over the content being sent. The best way to minimize creepiness was to have high control over the content being sent and high transparency. However, the book also noted that not all ads that were privacy intrusive were considered creepy (Book). Users in the smart home devices and online data collection studies reported targeted advertisements to be “creepy” and “weird”, respectively, but smart home users preferred targeted ads over irrelevant ads and users in online data collection studies were only temporarily bothered by targeted ads. Interestingly, receiving an ad that perfectly matches the users’ preferences was considered creepy. In news articles and the study on children’s perceptions of creepiness, participants expressed that technology that was “human-like” is perceived as creepy. On the other end of the extreme, if a user could not explain why they received a particular ad, that was also considered creepy. In the CRoSS study, they found that creepiness is negatively correlated with transparency, which is consistent with what the book addresses and controllability, which is consistent with concerns raised in the adaptive assistive technology and one of the online data collection studies.