EXPLORING PRIVACY IMPLICATIONS OF DEVICES AS SOCIAL ACTORS

by
Maxwell Keleher

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF SCIENCE

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
August, 2023

Abstract

The Computers Are Social Actors (CASA) paradigm proposes that users' interactions with computers follow the same social psychology principles as their interactions with people. CASA has potential value in guiding privacy design and research. Through an online survey, we found evidence that the CASA paradigm applies to privacy interactions with computers, smartphones, and digital assistants. Next, we conducted interviews following a grounded theory methodology to understand how CASA influenced privacy attitudes. CASA caused participants to either feel more comfortable sharing personal information with their device or to feel that their device invades their privacy. Whether CASA causes feelings of comfort or mistrust largely depends on participants' attitudes towards other related actors. To the best of our knowledge, this is the first study which explicitly explores CASA's relationship to privacy. We call for a systems theory approach to privacy design and research. Finally, we propose five CASA-influenced privacy design guidelines.

Acknowledgements

First and foremost, I would like to thank my supervisor, Dr. Sonia Chiasson. Thank you for all of your guidance over the past two years and for giving me opportunities to develop as a researcher. I am especially grateful that you tolerate my more esoteric ideas and shape them into something presentable.

I would like to thank the members of my thesis committee, Dr. Robert Biddle and Dr. Hala Assal. Thank you both for providing such valuable discussion and feedback. I would like to thank Dr. David Barrera for chairing my committee. Also, thank you very much to my participants for sharing their time, experiences, and opinions with me.

Thank you to all members of the CHORUS Lab; it has been a pleasure to get to know you all over the past two years. I feel incredibly fortunate to be surrounded by such generous and insightful peers. Thank you for pilot testing my studies, giving feedback on my presentations, and sharing all of your knowledge and experiences.

I am eternally grateful for the support my friends and family have given me throughout my academic career. Thank you for listening to me ramble about privacy and CASA, and getting me to step away from my thesis and go outside sometimes!

Finally to Arielle, thank you for your unending support throughout the past two years, and for keeping me grounded. Thank you for always listening to unpolished thoughts and for always being the first and loudest voice to celebrate my accomplishments! I cannot wait to see what our future holds!

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

> *When she's not plugged in, I referred to her as an it. When she's plugged in, I refer to her by her name. And it's like right now she's just [...] sitting there. [...] It's just [...] an appliance. But when she's plugged in, I think of her as a person mostly* (P5, Chapter 4 Interview Study).

1.1 Motivation

As technology proliferated, digital privacy has become more obviously intertwined with social and emotional phenomena. In fact, people have expressed some digital privacy concerns which are eerily similar to social, interpersonal concerns related to privacy. People worry their smartphones or their digital assistants are listening to them and sharing their private conversations with companies or advertisers [19, 45]. Since an invasion of privacy requires someone – or something – to do the invading, privacy is fundamentally linked to social interaction.

The Computers Are Social Actors (CASA) paradigm proposes that users' interactions with computers follow the same social psychology principles as their interactions with people [62]. The CASA paradigm is valuable both as an explanatory framework for how users interact with devices, as well as providing insights which can be leveraged to improve software usability. Nass described in his book *The Man Who Lied to his Laptop* [63] that he, since working on the original studies that revealed CASA, has used principles from CASA to improve the usability of customer satisfaction surveys and car navigation systems.

If CASA is applicable in privacy contexts, how might it have positive or negative influences on users? CASA has not been explicitly connected to privacy design, despite having been applied to improve digital designs and there being ways that social interaction influences digital privacy. We were not able to find any work that

specifically studies the relevance of CASA in the context of privacy.

As demonstrated in the examples from the opening paragraph, there has been a dramatic shift in the types of computing devices available to users since the original CASA studies from the early 1990s which used primarily desktop computers. Computers have become significantly more portable, more accessible, and more computationally powerful. Moreover, smartphones have become ubiquitous, but they only began to spread in usage across many parts of the world in the late 1990s [71]. The advancement of the internet has also shaped our usage of digital devices by providing platforms for social media and changing the ways we access information. Moreover, the connectivity of the Internet led to Internet of Things (IoT) devices such as digital assistants: stand-alone devices which house artificially intelligent personal assistants, which have become common household items.

Contemporary studies of digital privacy and CASA should account for the different ways that people interact with digital technology today. Therefore, we investigate three different devices: *computers* (desktops or laptops with which one can connect to the internet or complete basic computational tasks), *smartphones* (mobile computing devices which can connect to the internet, and can complete telecommunication tasks such as calling and texting), and *digital assistants* (artificially intelligent personal assistants which operate from their own dedicated hardware and NOT from a smartphone or computer – e.g. Google Home or Amazon Echo).

1.2 Research Questions

Because of the lack of research connecting CASA and privacy, we investigate whether CASA still holds true during privacy interactions. We address the following three questions across two studies:

RQ1 *In which privacy contexts, if any, is social agency attributed to each type of device?*

RQ2 *What differences, if any, exist in people's privacy attitudes towards each type of device?*

RQ3 *How, if at all, are people's privacy attitudes explained by CASA?*

To explore the relationship between CASA and privacy attitudes and behaviours, we first ran an online survey with 400 participants based on psychology privacy preference scales to identify whether CASA applies to privacy interaction contexts. Afterwards, we conducted interviews with 12 participants following a grounded theory methodology to build a theory of how people's privacy attitudes and behaviours are influenced by CASA. From these two studies, we derive a set of CASA informed privacy design guidelines.

1.3 Contributions

To the best of our knowledge, this research is the first to explicitly study and identify a connection between CASA and privacy attitudes. We found evidence of social agency for at least one of the three devices in four of the seven privacy themes (high-level privacy contexts used to group the related survey questions for our analysis). We also found significant differences in participants' privacy attitudes towards each of the three devices: attitudes towards digital assistants were different from participants' attitudes towards computers and smartphones.

From our grounded theory interview results, we found that CASA does, in fact, have an effect on privacy attitudes. We present a theory of how CASA influences participants' privacy attitudes towards their devices and describe the way that perceptions of other devices, other people, and brands shaped the effect of CASA on privacy attitudes.

In the discussion, we look to previous literature for possible explanations about these attitudes and behaviours, and then describe the value in taking a systemic design approach to privacy design. Finally, we propose a set of high-level privacy design guidelines making use of CASA for privacy design.

1.4 Thesis Outline

The remaining chapters of the thesis are as follows:

Chapter 2 We start by covering some key terminology used throughout the thesis. Then we describe the history of CASA research and the contemporary understanding of privacy attitudes and behaviours towards computers, smartphones, and digital assistants. We provide relevant context from social psychology; in particular highlighting the way that social behaviours relate to privacy. Finally, we point out the gap in research around CASA and privacy attitudes and behaviours.

Chapter 3 Then, we present our first study: an online survey with 400 participants. We use questions from psychology privacy preference scales which are modified to inquire about preferences in interactions with each of the three devices to search for cases where participants treat their devices as social actors.

Chapter 4 Next, we present our second study: a series of interviews following a grounded theory methodology. Our goal with this study was to develop a theory of how CASA explains privacy attitudes and behaviours with the three devices.

Chapter 5 In the final chapter, we reflect on the studies to address our research questions. We then suggest possible explanations for notable privacy attitudes and behaviours related to CASA. we also suggest that privacy design and research should adopt a systems thinking approach. Finally, we present a set of five CASA-informed privacy design guidelines.

Chapter 2

Background

2.1 Key Terminology

In this thesis, we use terminology from both social psychology and from privacy research. Below, we define the terms we use in this thesis.

Actor: An actor is an entity that can *do* something [38]. Actors include humans, non-human objects, and groups (such as communities or organizations) [38]. This definition is used in Actor-Network Theory. In other words, an actor is anything capable of interacting with another actor. The actors referenced in this thesis include humans, devices, groups of humans, and organizations (such as companies or brands).

Social Agency: Based on Nass et al.'s 1994 paper, an actor possesses social agency if you have a social response to it [62]. Humans obviously have social responses to each other, and the novel discovery by Nass et al. is that humans have social responses towards computers.

Privacy: Privacy is "the claim of an individual to determine what information about [themself] should be known to others" [84]. A high desire for privacy would generally mean that you are uncomfortable sharing sensitive information with others.

Trust: A person is considered trustworthy if you believe that they will engage in actions that benefit you or at the very least not engage in action that would be detrimental to you [32]. When you consider another person to be trustworthy, you feel more comfortable interacting and collaborating with them [32]. Consequently, you consider a device trustworthy if you feel that it benefits you or at least is not detrimental to you [49].

Computer: A desktop or laptop with which you are able to connect to the internet or complete basic computational task such as word processing (e.g. Desktop PC, Macbook, Dell Laptop, etc).

Smartphone: A portable computing device which is able to accomplish telecommunication tasks such as calling and texting as well as connect to the internet (e.g iPhone, Blackberry, Samsung Galaxy, etc).

Digital Assistant: An artificially intelligent assistant which operates from its own dedicated hardware and NOT from a smartphone or computer (e.g. Amazon Echo, Google Home, Apple Home Pod, etc).

2.2 Privacy Attitudes

Historically, much of the research into privacy attitudes and behaviours revolved around a "privacy paradox": a phenomenon where there is a dissonance between participants' stated privacy concerns and their lack of behavioural change to address their concerns [3,11,34,36,64]. More recent work questions the validity of the privacy paradox. A longitudinal study demonstrated that people do tend to share less information over time if they express concerns [25], and Solove argues that participants are explaining broad perceptions and attitudes which are being compared to specific behaviours [76]. Generally, people's digital privacy preferences are shaped more by the context in which the information is being asked rather than who is asking for the information [48]. Moreover, privacy attitudes can be shaped by institutional assurances such as privacy policies [87].

Generally, the concerns around smartphones include surveillance, intrusions, and (mis)use of personal data [37,42,46,88]. People who use their smartphone often seem to have less concern about privacy than those who use their smartphone less often [2]. Moreover, the users of different smartphone types (Apple vs Android) did not present significantly different concerns [2, 12]. The limited features for privacy control on smartphones prevent participants from expressing their true privacy concerns [40,66]. People share the most information when they lack details about how the data will be

used [73] and reactions to privacy violations tend to change based on perceived risk: lower risk violations are seen as mere annoyances rather than actual threats [27].

Study of end-user privacy attitudes and behaviours towards IoT devices, including digital assistants, has been particularly prominent in the past few years as such devices have become more accessible to consumers. Based on previous research, users seem to have incomplete mental models and threat models of digital assistants [1], and users tend not to take action though they voice privacy or security concerns [35]. A study about digital assistant adoption found that, generally, participants did not adopt the devices because they did not see utility from the device and only seven percent of participants raised security or privacy concerns [51]. Users have expressed concerns about how the digital assistants collect voice data (i.e, when the digital assistants are "listening") and how the voice data is used after it is collected [31, 51]. Park et al. [65] find that coping behaviours for privacy threats from digital assistants can cause negative emotional responses such as anger. Additionally, Lutz and Newlands [54] found that, though many participants may not have a high level of concern towards digital assistants themselves, they express privacy concerns about the companies which manufacture the devices.

2.3 Social Aspects of Privacy

A. Westin [84] defined privacy as "the claim of an individual to determine what information about [themself] should be known to others". In a 2003 paper [85], he expanded his definition of privacy by incorporating the social and political dimensions of privacy. He explains that a person's ability to "claim freedom from the observation of others" is shaped by "environmental factors such as crowded cities and class factors of wealth and race." Moreover, "a society considers a given mode of personal behavior to be socially acceptable – whether it is hairstyle, dress, sexual orientation, political or religious belief, having an abortion, or other lifestyle choice – it labels such conduct as a private rather than a public matter." Even from his first definition, the notion that one is determining what is known about themself to another implies that privacy is fundamentally related to social interaction. His expanded definition makes it even more clear that privacy as a concept is wrapped up in social interactions since privacy

is so fundamentally related to one's interactions and relationships with other people.

This connection between social issues and privacy also appears in digital privacy literature. For example, in a 2011 paper, boyd and Marwick [14] find that teenagers' ostensible lack of concern for privacy online reflects the lack of physical public space where teenagers can socialize. They argue that, in the absence of accessible public spaces, social media sites afford teenagers the space to develop socially. Additionally, Fahey and Hino [26] describe the conflict between collecting personal data for COVID-19 contact tracing, and individuals' desire for privacy. In this case, contact tracing applications come in conflict with social hurdles, most visibly a society's trust towards and compliance with their government.

A particularly prominent social theory connected to privacy is the Fear of Missing Out (FOMO). FOMO is defined as "a pervasive apprehension that others might be having rewarding experiences from which one is absent" including "when such information will be obtained and what uses will be made of it by others" [69]. The apprehension refers to "the desire to stay continually connected with what others are doing." F. Westin and Chiasson [86] found that FOMO can drive people to reluctantly adopt privacy compromising behaviours. Moreover, Milas and Lesinger [59] find that there is a correlation between one's level of privacy concern and their level of FOMO.

Clearly, there are several ways in which social issues and theories relate to digital privacy. Considering all of the ways that social issues connect to privacy, and A. Westin's definition addressing the way someone chooses to either share or hide information from others, it would appear that privacy is part of social interactions. Therefore, digital privacy would be a part of interaction with computing devices. Notably, there is existing research in the field of Human-Computer Interaction (HCI) demonstrating that interactions with devices are social interactions; we discuss this research in the subsequent sections.

2.4 Computers Are Social Actors (CASA)

CASA research stems from the studies summarized in Reeves and Nass' 1996 book, *The Media Equation*, in which they found that people's interactions with media followed the same social psychology principles as their interactions with people [70].

Where *The Media Equation* deals with media more broadly, CASA focuses specifically on interactions with computers. In their 1994 paper, Nass et al. [62] specifically addressed the CASA paradigm and explained it as a phenomenon where humans apply social interaction norms when interacting with their computer [62].

The general method of studies in *The Media Equation* involved modifying social psychology studies, which demonstrate a social behaviour, by replacing the researcher-controlled participant with a computer to see if the social behaviour appears in interactions with computers [70]. In "Computers are Social Actors", Nass et al. [62] report on five of these studies which all follow the same general method: researchers told participants that they would complete a test after a computerized tutoring session. The first of their five studies concluded that participants are polite towards computers. Participants completed evaluations of a computer's tutoring ability with either the same computer that tutored them, a different computer, or using pen and paper; in the end, participants provided more favourable evaluations when responding on the computer being evaluated. In study two, they identified that participants attribute notions of "self" and "other" in how they perceive a computer's praise and criticism of itself and others. Study three expands upon the way people apply notions of "self" and "other" to computers by highlighting that participants identify voices as unique actors and recognize a repeated voice as the same actor. The fourth study found that participants "apply gender stereotypes" to computers based on the perceived gender of a computers voice. The fifth study demonstrated that participants attribute social agency to the computer itself and not to another agent through the computer. Nass et al. present these results not as dysfunctional behaviour, but rather a demonstration that interactions between humans and computers are fundamentally social. They argue that these finding indicate that "social psychology, communication, and sociology" are all relevant to the field of HCI and have "clear implications" for the design of user interfaces.

Nass and Moon explain the theory of CASA as a case where people apply *human-human interaction* scripts to their interactions with computers [61]. In this case, they use scripts to refer to "social scripts" which are frequently and predictably repeated social behaviours. Gambino et al. return to this concept of social scripts to address

the changes that have occurred since the original CASA studies [33]. They argue that given the length of time humans have now had interacting with various computing devices, people may have developed *human-device interaction* scripts. Therefore, they call for future research to investigate when people apply human-human scripts to interactions with devices and when they apply human-device scripts.

The early CASA studies only investigated interaction with desktop computers. Subsequent studies have explored how this paradigm applies to devices or technologies including smartphones [15–17] and voice assistants [58]. Other studies have demonstrated that CASA manifests in specific contexts (e.g., with children [21], or in online journalism [50]). Given the significant changes in technology and how humans interact with said technology, researchers such as Gambino et al. [33] and Lombard and Xu [53] have sought to update the paradigm to reflect the current technology landscape by studying more modern devices or applying new methodologies. However, we found no studies that explicitly apply or investigate the CASA paradigm in relation to digital privacy.

2.5 CASA and Privacy

One possible connection between CASA and privacy is through the concept of trust towards a device. Studies by Lee and Nass [49] demonstrate the relevancy of CASA in building trusting relationships between humans and computers in three key ways. First, Lee and Nass studied effect of similarity between the participant and the computer on the participant's trust towards the computer. Lee and Nass used computer-synthesized voices to have computers "talk" to participants and match the participants' level of introversion or extroversion; extroverted participants expressed more trust towards computers that acted like extroverts and introverts were more trusting of computers that acted like introverts. Second, they studied the effect of "caring behaviours". Participants were more trusting of computers that displayed "empathetic emotions" even though computers are "lifeless artifacts" unable to express "genuine feelings". Third, they found that participants were more trusting of computers which were "consistent" in their "humanness". Participants expressed more trust towards a computer which adopted a recorded, human voice **and** referred to itself with "I"

or "me", compared to when it used one of the two features **without** the other. Similarly, participants were more trusting of computers that adopted a human face and a human voice as opposed to those that adopted human voice without a human face (or vice versa).

In *Privacy as Trust* [83], Waldman explains that trust is at the core of one's decision to disclose sensitive information with someone else. She further explains that invasions of privacy manifest as a breach of trust: trust in another makes one comfortable disclosing sensitive information and so leaking of that information indicates that one's trust was misplaced. These points complement Gambetta's definition of trust [32], "we trust someone [who] will perform an action that is beneficial or at least not detrimental to us" – which is the definition cited by Lee and Nass' [49]. According to Lee and Nass, people "perceive computers [as] trustworthy" when they "[expect] that the computers would be 'beneficial' or at least 'not detrimental to us'." Based on Waldman [83], people need to trust a device to disclose to it sensitive information, and could feel that the device has broken their trust if it leaks confidential information.

Following Lee and Nass' work about CASA and trust, there have been several studies which have sought to understand how users trust IoT devices, including digital assistants, [9, 10, 29, 52, 68, 74] but these studies have not sought to establish any explicit connections between CASA and privacy.

There are some cases where research ostensibly indicates a connection between CASA and privacy but does not explicitly link the two topics. An example is Kitkowska et al.'s [43] 2020 study where they improved privacy notices through designing for a positive emotional effect, but they did not explicitly position their work through a CASA lens. On the other hand, Alberts and Van Kleek's 2023 paper, "Computers are Bad Social Actors: Dark Patterns and Anti-Patterns in Interfaces that Act Socially", shows how certain applications exploit social behaviours to manipulate users into certain actions [6]. They then present guidelines, such as respecting a user's personal boundaries, to avoid interface designs which exploit social behaviours.

2.6 Privacy Preference Scales

Like trust scales, privacy scales are the most common methodology for quantitatively studying privacy attitudes. A scale is typically presented to participants as a series of Likert-style multiple choice questions which ask participants to indicate their agreement with statements related to privacy. In their 2022 study, Colnago et al. [22] raised concerns about the wording of several popular privacy scales in digital privacy literature by pointing out that they overly focus on concerns about privacy rather than more generalized feelings. Beyond this criticism about limitations of the language, scales such as the Internet Users' Information Privacy Concerns (IUIPC-10) or Concern For Information Privacy (CFIP) scales focus on information and data in ways that make it difficult to adapt them to study social situations; thus making them inappropriate for a CASA study [56, 75].

As further detailed in Section 3.1, we have instead opted to adapt privacy preference scales from social psychology literature. This approach is in keeping with the general approach of the original CASA studies, modifying social psychology studies to replace interactions with humans to interactions with devices. Though there have been scales proposed to measure trust – both scales for trust between humans and computers [55] and more general trust attitudes [89, 90] – we look to scales which cover broader privacy attitudes in order to fully explore the possibility of CASA in privacy contexts. Acknowledging criticisms in Colnago et al.'s study [22], we sought out scales which refer to privacy attitudes more broadly rather than focusing on just privacy concerns.

Marshall's Dimensions of Privacy Preferences [57] First, we look to the foundational privacy preference scale in social psychology published by Marshall [57] in 1974, as part of a larger project to study the relationships between suburban young adults and their parents. The scale contains 56 questions generated from "interviews with university undergraduates, from written accounts of privacy conflicts and adaptations to them made by various populations [found in the literature], and from theoretical considerations." Each item in the scale is presented as a statement and respondents select from Likert-style responses ranging from "strongly agree" to "strongly

disagree". Through principle axis factor analysis, Marshall identified 6 factors to group related scale items: intimacy, comfort sharing personal facts with an intimate person or family member; not neighbouring, avoiding spending time or sharing personal facts with neighbours; seclusion, being isolated from others by sight and sound; solitude, being physically or mentally alone; anonymity, being able to attain privacy by others not knowing "everything about you"; low self-disclosure, preference to disclose little about oneself to other.

Pedersen's Dimensions of Privacy [67] In 1979, Pedersen published his own privacy preference scale. Pedersen wished to develop a scale that addressed A. Westin's four types of privacy [84]: "solitude, person is alone and free from observation by others; intimacy, a group maximizes interpersonal relationships by minimizing outside surveillance; anonymity, person is surrounded by others but does not expect to be recognized; reserve, person withholds personal aspects of [themself] from others." Pedersen's scale development unfolded in two phases. In phase one, Pedersen and two assistants generated 96 questions which were administered as 6-point Likert scale questions with the options being: never, rarely, occasionally, sometimes, often, and usually. In phase two, Pedersen used factor analysis to refine the original question pool to 30 questions and modified the questions to be presented as statements like in Marshall's scale. Pedersen's results add some detail to A. Westin's four types of privacy. First, he found two types intimacy: with friends and with family. Second, he identifies a desire for isolation which is separate from a desire for solitude claiming "a person who likes to be alone in a bedroom or study may not like being alone in a remote area." Unlike Marshall, Pedersen did not organize his scale by the factors revealed in factor analysis.

Craddock's Relationship Privacy Preference Scale [23] Craddock's scale, published in 1997, references both Marshall's and Pedersen's scales. However, Craddock specifically investigates privacy attitudes in marital relationships rather than privacy attitudes in general. Craddock set out to develop a scale which covered four categories: "neighbour avoidance, preference for avoidance of contact with neigbours; solitude, preference for time to be alone even from, partner; reserve with partner,

preference for low self-disclosure with partner; possessiveness, preference to reserve things and territory for personal use". Craddock started with an unspecified number of questions, each related to one of the four categories, that followed a 5-point Likert format of presenting a statement and response options ranging from strongly disagree to strongly agree. Through confirmatory factor analysis, Craddock derived a final 12-item scale. He finally he field tested the scale with 106 participants to confirm that it possesses a sound factor structure, is reliable, and has predictive validity.

2.7 Summary

Privacy as a concept is intrinsically linked to social interactions. Consequently, much research about digital privacy has brought up or has been related to concepts from social psychology. Fortunately, there is an theory which explicitly demonstrates that interactions with computers are social interactions, Computers are Social Actors (CASA). Moreover, the concept of trust, a core component of privacy attitudes, has been explored in relation to CASA. However, we have been unable to find research which explicitly connects privacy and CASA, or even seeks to understand whether such a connection exists. In this thesis, we investigate how privacy interactions fit into the CASA research area, and how CASA influences privacy attitudes and behaviours.

We used two studies to address this gap in understanding around CASA and digital privacy. First, we needed to understand whether CASA holds true in privacy interactions. Second, we sought to understand how participants' privacy attitudes and behaviours are influenced by CASA.

Chapter 3

Survey Study

The first step of our research was to determine when, if at all, participants' privacy interactions follow human-human interaction scripts. For reasons we explain below, we used an online questionnaire. This questionnaire addresses the first two research questions in this thesis:

RQ1 *In which privacy contexts, if any, is social agency attributed to each type of device?*

RQ2 *What differences, if any, exist in people's privacy attitudes towards each type of device?*

In this chapter, we outline our methodology for conducting this questionnaire study. Then we describe our results, and finally, we interpret the results in relation to the research questions.

3.1 Methodology

Carleton University's Research Ethics Board reviewed and provided clearance for the study. As we were studying the presence of social agency, we followed a similar methodology to the original CASA studies. Our general approach involved asking participants questions from psychology privacy scales relating to another person, and asking a second version of each question referring to either computers, smartphones, or digital assistants. we obtained consent from all participants prior to their participation in any survey.

Our study followed a mixed design. For both research questions, the dependent variables were the 5-point Likert-scales. We used a within-group design to answer RQ1. The independent variable was which *actor* was used in the question: a person

or device. A survey contained questions about the *device* (one of: computer, smartphone, or digital assistant) and matching questions about another *person*. The device questions presented to a given participant consistently referred to a single device (one of: a computer, smartphone, or digital assistant). For example, one participant would be asked questions about a *computer* and a person. A correlation between a participant's responses to the two versions of questions would indicate social agency for that device. For RQ2, we used a between-group design where the independent variable was the *type of device* mentioned in the question – either *computer*, *smartphone*, or *digital assistant*.

Our methodology differs from the original CASA studies in that it relies on questionnaires rather than lab studies. To the best of our knowledge, privacy preference scales are the primary methodology for studying privacy in psychology studies. Therefore, we believe that our methodology aligns with the guiding principle of the original CASA methodologies, which is taking existing social psychology protocols and running them with a computer in place of the social actor.

3.1.1 Survey Design

The survey included one set of 45 questions about privacy attitudes toward people and a matching set of 45 questions relating to a given device. To avoid ordering bias, we presented the questions in pseudo-random order, with restrictions preventing participants from encountering the matched questions immediately following each other. To avoid acquiescence bias, several pairs of person and device questions were reverse-coded[1], with matching pairs always remaining in the same direction. We hosted the survey on Qualtrics[2] and we have included a copy of the questionnaire in Appendix A. We ran two rounds of pilot testing: one with lab members to check that the questions made sense in both the device and person formats, which resulted in some rewording, and the second with five participants on Prolific.

Recruitment materials and the survey introductions stated that we were surveying participants about their perceptions of different devices, with no explicit mention of

[1]The questions were already reverse-coded in the original scales

[2]`https://www.qualtrics.com/`

privacy or CASA. At the end of the survey, we included a debrief to explain why they were asked similar questions twice.

Question Generation

We referenced three established privacy attitude scales to construct our survey: Craddock's [23], Marshall's [57], and Pedersen's [67]. Since we were unsure how (or if) participants' relationships with devices in privacy contexts map onto interpersonal relationships, we chose these three scales covering several different types of relationships (friends, neighbours, spouses, etc.). We took questions which could be minimally altered to reference computers, smartphones, and digital assistants. Below is an example of how we changed the wording to make matching pairs of questions. The person version of the question comes from Marshall's scale and is part of our *Intimacy* privacy theme. The version which concerns a device was modified to replace the referenced person with one of: "computers", "smartphones", or "digital assistants":

Person: Even intimate friends should respect your desire to keep certain things to yourself.

Device: Even personal *computers/smartphones/digital assistants* should respect your desire to keep certain things to yourself.

Privacy Themes

Both Craddock and Marshall organized their questions into privacy themes [23, 57] using exploratory factor analysis; Pedersen's privacy scale had no question grouping [67]. We kept questions from Marshall's and Craddock's scales in their original grouping and we moved the questions from Pedersen's scale into the most appropriate theme. We verified the placement of questions from Pedersen's scale using confirmatory factor analysis – which we detail below.

We summarize our final set of themes and their definitions in Table 3.1. The *Solitude* theme was shared between Marshall's and Craddock's scales so we merged these questions under a single theme and added questions from Pedersen. *Intimacy*,

ID	Theme	Device Description	Person Description	N	RMSEA
IN	Intimacy	Preference to use a personal device over other devices and the ability to trust personal devices with sensitive information; in other words, including the device in one's intimate social 'bubble'.	Preference to spend time with only intimate friends, partners, or family instead of time with others and the ability to trust these individuals with confidential information; in other words, including the individual in one's intimate social 'bubble' [57].	7	0.088
NN	Not neighbouring	Preference to avoid contact with devices.	Preference to avoid contact with neighbours [23].	3	0
SO	Solitude	Preference to have time physically and mentally alone even from personal devices.	Preference to have time alone even from intimate friends, partners, or family including time alone mentally while others are nearby [23, 57].	7	0.057
AN	Anonymity	Preference for non-personal devices not to know much about one's self.	Preference for one's community not to know information about oneself [57].	2	–
LD	Low-self disclosure	Preference to disclose little information about oneself to devices.	Preference to disclose little information about oneself [57].	5	0.073
RP	Reserve with partner	Preference to disclose little information about oneself even to personal devices.	Preference to disclose little information about oneself even with one's partner [23].	3	0
PO	Possessiveness	Preference to keep items or spaces for personal use rather than share them with devices.	Preference to keep items or spaces for personal use rather than share them with others [23].	2	–

Table 3.1: Privacy themes grouping the survey questions for analysis. Each theme was originally defined in the corresponding psychology scale papers for interaction with a person; we also describe how the theme applies to human-device interactions. N = the final number of questions per theme after confirmatory factor analysis. Root mean square error of approximation (RMSEA) = results for Round 2 confirmatory factor analysis; RMSEA < 0.1 are considered a reasonably good fit. A full list of the questions within each theme is available in Appendix A.

Seclusion, *Anonymity*, and *Low-Self Disclosure* contain questions from both Marshall's and Pedersen's scale. Our *Not Neighbouring* theme is composed exclusively of questions from Marshall's scale. *Reserve With Partner* and *Possessiveness* are made up exclusively of questions from Craddock's scale. Our process for arriving at this final set of themes and questions follows.

Factor Analysis Round 1 We started with 45 questions across eight themes. We performed confirmatory factor analysis (CFA)[3] on the set of questions referencing people to ensure that we appropriately categorized the questions from Pedersen's

[3]CFA was computed in R with the `cfa` function from lavan (version 0.6-15)

scale; adjustments were necessary. One theme (*Seclusion*) was a very poor fit so we discarded it. We excluded several other questions due to poor fit and poor phrasing: four from *Intimacy*, one from *Not neighbouring*, two from *Solitude*, one from *Anonymity*, one from *Low-self disclosure*, and one from *Possessiveness*. The *Seclusion* theme, which was discarded, contained 6 questions. In Appendix A, we highlight the questions which were excluded from analysis by highlighting them in red.

Factor Analysis Round 2 We ran a second round of confirmatory factor analysis on the 29 questions that remained after adjusting based on the first round. The *Anonymity* and *Possessiveness* themes are comprised entirely of questions from the original scales (Marshall's and Craddock's respectively). Therefore, they had already been validated in original studies. We ran a second one-factor analysis for the five remaining themes, each of which had three or more questions. All five themes had root mean square error of approximation (RMSEA) values of < 0.1 (see Table 3.1) indicating at least a *reasonably good fit* according to the cutoff criteria described by Kline [44]. We also ran a confirmatory factor analysis for all three device question sets: RMSEA for all the devices was less than the threshold, < 0.1 (computer is RMSEA of 0.087, smartphone is 0.088, and digital assistant is 0.085). Therefore, we are confident that we had appropriate groupings for the survey questions.

Common Method Bias Test We used Herman's single factor approach to test for common method bias. We found the portion of variance explained to be < 0.5 (in this case, the proportion of variance explained is 0.13) which indicates that there was not common method bias in the results.

Final set of questions and themes After two rounds of factor analysis, we were left with 29 questions across the seven themes described Table 3.1. All further analysis is based on these seven themes.

3.1.2 Recruitment and Participants

We used the UK-based crowd-sourcing platform Prolific[4] to recruit participants. Participants had to be at least 18 years old, currently reside in Canada, and be able to read and complete a survey in English. Based on Prolific's suggested payment rates, we paid participants 1.34 GBP (approx. 2.09 CAD) upon completion of the survey.

We took advantage of Prolific's screening questions to ensure that participants were assigned to a study condition for a device with which they had experience. The participants for the digital assistant group self-described having experience with "internet enabled products: Home assistants/smart hub (e.g. Amazon Echo, CastleHub, Google Home)". As there was no finer granularity available with Prolific, the smartphone and computer participants self-described having experience with "devices with screens: Mobile Phone, Laptop, Desktop". Within the survey, we asked more specific demographic questions to ensure the participants had the appropriate experience with either computers, smartphones, or digital assistants.

3.1.3 Data Collection

We collected our data in August 2022. On Prolific, six participants timed-out so their responses were discarded. Qualtrics monitors responses for suspiciously fast completion, multiple submissions from single participant, and possible bots. None of the responses were flagged. In the end, we received 401 responses which were not automatically rejected or flagged. During manual data cleaning, we excluded one participant from the smartphone group because they only answered the demographic questions, leaving 400 valid responses for analysis. After cleaning, we had 144 responses for the *computer* group, 127 responses for the *smartphone* group, and 129 responses for the *digital assistant* group.

Demographics Participant demographics are available in Table 3.2; their self-reported knowledge of technology and device usage are summarized in Table 3.3. Generally, there was faster median completion time and higher tech literacy reported

[4] `https://www.prolific.co/`

Group	Women	Non-Binary	Men	Prefer not to answer	Median Age	Median Completion Time (mm:ss)
Computer	79	6	59	0	35	11:15
Smartphone	67	1	58	1	32	10:51
Digital Assistants	74	2	54	0	31	10:15
Overall	220	9	171	1	32	10:45

Table 3.2: Demographic information for survey participants

	Knowledge of technology				Frequency of use			
Group	Basic	Intermediate	Advanced	Proficient	Every day	4-6 days a week	2-3 days a week	Once a week
Computer	5	23	91	25	132	10	2	0
Smartphone	1	16	90	20	125	0	1	1
Digital Assistants	0	4	91	35	63	28	27	11
Overall	6	43	272	80	320	38	30	12

Table 3.3: Self-described knowledge of technology and frequency of using the device.

for participants in the *digital assistant* group. They also reported less frequent usage of their device than participants from the other two groups.

3.2 Analysis

We analyzed the survey responses in two phases, addressing each of our research questions. We first address *RQ1: In which privacy contexts, if any, is social agency attributed to each type of device?* by looking for *within-subjects* correlations. For each of the seven themes, we determined an aggregate *device* score per participant by taking the mean of all the questions in the theme. We followed the same procedure to determine an aggregate *person* score. For example, a participant's aggregate score about another person for the `Low-self disclosure` theme would be the mean of their responses to the five questions about another person in the theme. In the end, each participant had an aggregate score for each actor per theme – in total, seven aggregate scores about the device and seven aggregate scores about another person. We used Kendall tau rank correlation coefficient tests to look for relationships between participants' aggregated scores for the device questions (computer, smartphone, or digital assistant) and the matched person questions for each of the privacy themes. We

used Kendall's tau-b, a non-parametric test measuring the strength of the association between two sets of ordinal data, because there were many ties between participants in the aggregate scores [4]. We interpret correlations between the device and person questions as evidence of social agency in relation to the given privacy theme.

To address *RQ2: What differences, if any, exist in people's privacy attitudes towards each type of device?*, we ran one-way non-parametric Kruskal-Wallis tests to look for differences in how participants responded to the questions about the three computing devices. We then use pairwise Dunn tests for post hoc analysis.

We corrected for multiple statistical tests using the Holm-Bonferroni method. Holm-Bonferroni adjusts the p value directly so we used $\alpha = 0.05$ to reject null hypotheses. We corrected the correlation tests to account for 21 tests and Kruskal-Wallis tests to account for seven tests; we applied family-wise corrections to the Dunn tests by device pairing (accounting for seven tests each).

3.3 Results

In the subsequent sections, we first provide an overview of how participants responded to questions about people and the three devices. Then, we address RQ1 and RQ2 through statistical analysis of the data.

3.3.1 Survey Responses

In Table 3.4, we provide aggregate descriptive statistics per theme. For more detail, the boxplots in Figure 3.1 illustrate the distributions per question, ordered by theme. Before addressing our research questions, we provide a brief overview of the data, noting broad trends from visual observation; statistical comparisons are provided in the later sections. For six of the themes (NN, SO, AN, LD, RP, and PO), all except for *Intimacy*, higher values for the Likert scale responses indicate a higher desire for privacy *from* the social agent (i.e., device or person) – and a lower value on the Likert scale indicates a lower desire for privacy.

For the *Intimacy* theme, higher response values indicate an expectation that participants can *trust* the social agent (i.e., device or person) and that shared information with be kept *confidential* (i.e., forming an private social 'bubble'). A lower response

		Median		Mean (SD)		Correlation		
Theme	Group	Device	Person	Device	Person	Tau	p value	Z value
IN	Computers	4	4	3.4127 (1.32)	4.2321 (0.87)	0.1280	0.3793	2.1144
	Smartphones	4	4	3.3948 (1.27)	4.2632 (0.83)	**0.2494**	**0.0017**	**3.8602**
	Digital Assistants	3	5	2.8396 (1.48)	4.3760 (0.80)	0.0426	1.0000	0.6625
NN	Computers	3	3	3.3866 (1.16)	2.9352 (1.19)	-0.1313	0.3793	-2.0933
	Smartphones	3	3	3.3438 (1.15)	2.7816 (1.10)	0.0108	1.0000	0.1596
	Digital Assistants	4	2	3.8333 (1.09)	2.7897 (1.22)	0.0065	1.0000	0.0985
SO	Computers	2	4	3.2649 (1.20)	4.0357 (1.00)	**0.2086**	**0.0060**	**3.5042**
	Smartphones	3	4	3.3863 (1.13)	3.9516 (1.04)	**0.2642**	**0.0006**	**4.1490**
	Digital Assistants	4	4	3.6185 (1.10)	4.0804 (0.96)	**0.2939**	**< 0.0001**	**4.6210**
AN	Computers	3	3	2.7247 (1.23)	3.3090 (1.06)	**0.2571**	**0.0012**	**3.9503**
	Smartphones	3	3	2.6024 (1.14)	3.4134 (1.08)	**0.2630**	**0.0022**	**3.7779**
	Digital Assistants	2	4	2.1931 (1.17)	3.5212 (1.06)	0.1683	0.1831	2.4261
LD	Computers	4	4	3.5653 (1.17)	3.9028 (1.08)	**0.3153**	**< 0.0001**	**5.2016**
	Smartphones	4	4	3.6961 (1.08)	4.0457 (1.00)	**0.2859**	**0.0002**	**4.4093**
	Digital Assistants	4	4	3.8470 (1.15)	3.9877 (1.13)	**0.2617**	**0.0010**	**4.0160**
RP	Computers	4	2	4.0255 (1.00)	2.3704 (1.11)	-0.0383	1.0000	-0.6084
	Smartphones	4	2	4.1207 (0.98)	2.3963 (1.18)	0.1399	0.3793	2.0790
	Digital Assistants	5	2	4.4267 (0.86)	2.0641 (1.08)	-0.0540	1.0000	-0.7821
PO	Computers	4	2	3.4826 (1.17)	2.5174 (1.18)	-0.0174	1.0000	-0.2684
	Smartphones	4	2	43.6772 (1.24)	2.5787 (1.16)	-0.0248	1.0000	-0.3601
	Digital Assistants	4	2	3.7375 (1.33)	2.2692 (1.12)	0.0539	1.0000	0.7887

Table 3.4: Mean, median, standard deviation, and Holm-Bonferonni adjusted correlation results between *people* and each device group per privacy theme. Items in bold with blue background are statistically significant.

indicates an understanding that interactions with the social agent (device or person) may be shared.

Person Questions Participants' responses to the person questions generally leaned towards the more private end of the scale for the *Intimacy* (IN), *Solitude* (SO), and *Low-self disclosure* (LD) themes. These responses indicate that participants generally desired privacy from other people, but also had a preference for forming social bubbles with intimate friends or partners.

Responses to the person questions were generally more neutral, relative to the other themes, in the *Not neighbouring* (NN) and *Anonymity* (AN) themes. This suggests that participants were neutral about privacy from their community.

The person question responses for the *Reserve with partner* (RP) and *Possessiveness* (PO) themes indicate less desire for privacy than the other themes, suggesting that the participants were generally comfortable disclosing sensitive information with

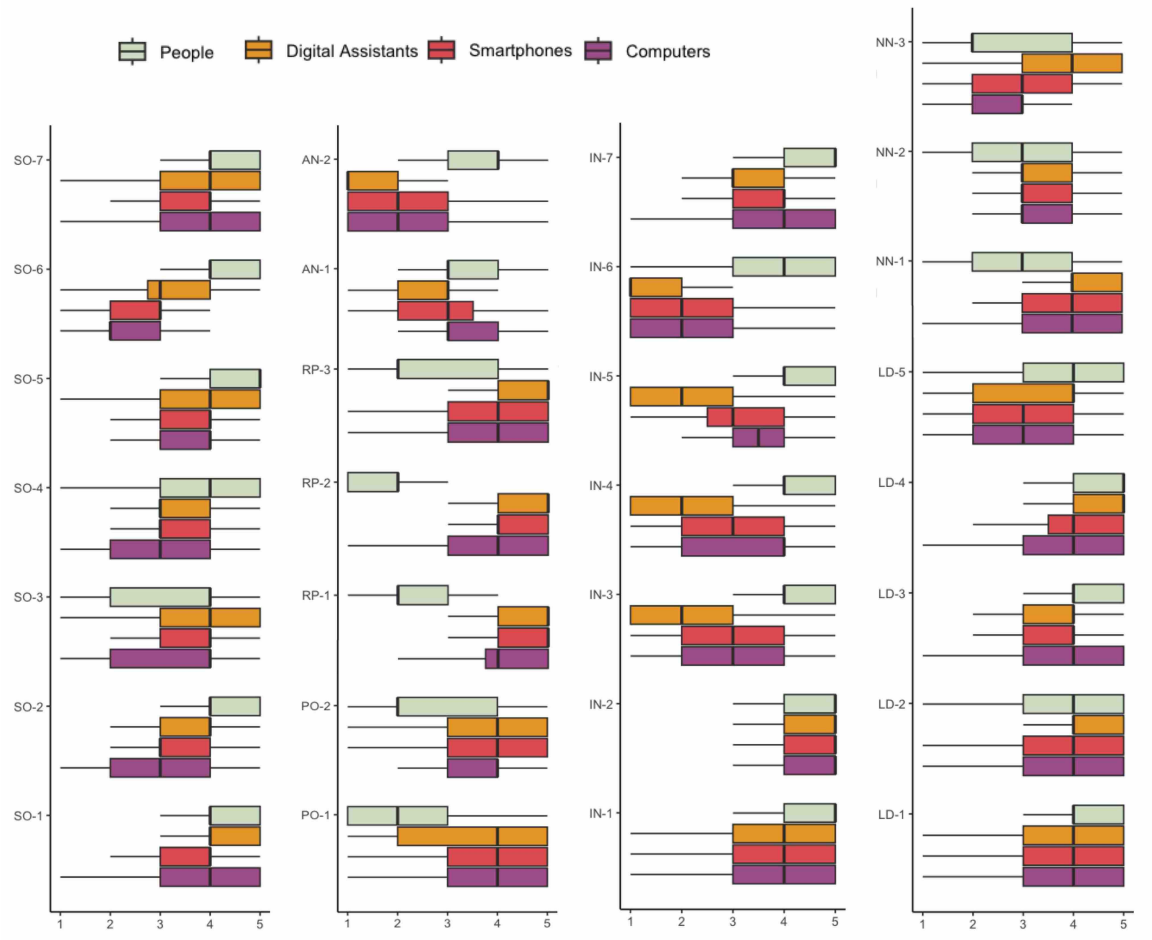

Figure 3.1: Likert scale responses per question, organized by theme. 1 = least desire for privacy, 5 = most desire for privacy from the given device or person.

intimate partners and sharing items or physical space with them.

Device Questions In four of the seven themes (SO, RP, PO and NN), the computers and smartphones responses were similar to the responses to the person questions, while responses for digital assistants differed. In the *Solitude* (SO) theme, the computer and smartphone responses were slightly lower than their matched person responses. This suggests that participants may be more neutral about the presence of a computer or smartphone, versus another digital assistant or another person, when they wanted to be alone. All device responses were higher than their matched person responses for the *Reserve with partner* (RP) and *Possessiveness* (PO) themes. These results indicate that participants may be less comfortable sharing information, items,

or physical space with the a device than they were with another person. It could also show that participants may not treat relationships with devices as close, intimate relationships.

The digital assistant responses were higher than their matched person responses for the *Not neighbouring* (NN) theme and were lower in the *Intimacy* (IN) theme, both of which indicate that that digital assistants may not be part of a trusted social bubble. The digital assistant responses for the *Anonymity* (AN) theme were also lower than their matched person responses which suggests that participants were more comfortable with an unfamiliar digital assistant knowing information about them than a stranger.

3.3.2 RQ1: Effect of *actor*

We used Kendall's tau rank correlation coefficient[5] with Holm-Bonferroni adjustment[6] to look for correlations between the means of the device responses and the person responses per theme. According to van den Berg [81], $tau > 0.07$ signifies a weak correlation, $tau > 0.21$ is the threshold for a medium correlation, and $tau > 0.35$ is the threshold for a strong correlation.

As shown in Table 3.4, we found statistically significant correlations between the device questions and the people questions in four of the seven privacy themes. We interpret a correlation to indicate that participants attributed social agency to the given device in the context represented by the privacy theme. The correlation simply indicates a relationship between the device and person responses, not necessarily a high or low desire for privacy.

Two themes, *Solitude* and *Low-self disclosure*, had correlations between device and people questions for all three devices. Our results indicate medium correlations in every case except for the computers group in the *Solitude* theme, which has a weak correlation (tau = 0.2086). Additionally, the *Intimacy* theme has a medium correlation for the smartphone group and the *Anonymity* theme had medium correlations for the computer and smartphone groups. We found no correlations for the

[5]Correlation tests were computed in R with `corr.test` function from psych (version 2.2.6)

[6]Holm-Bonferroni adjustments were computed in R with the `p.adjust` function from stats (version 3.6.2)

	Kruskal-Wallis Test		Dunn Test			
Theme	Chi Squared	p Value	D-C	S-C	S-D	Relationship
IN	**78.3459**	**< 0.0001**	**< 0.0001**	1	**< 0.0001**	$D < C\&S$
NN	**34.9543**	**< 0.0001**	**< 0.0001**	1	**< 0.0001**	$D > C\&S$
SO	**15.5752**	**0.0012**	**0.0003**	1	**0.0329**	$D > C\&S$
AN	**23.4368**	**< 0.0001**	**< 0.0001**	1	**0.0011**	$D < C\&S$
LD	**10.7583**	**0.0092**	**0.0021**	1	0.1222	$D > C, D \approx S, C \approx S$
RP	**24.2611**	**< 0.0001**	**< 0.0001**	1	**0.0011**	$D > C\&S$
PO	**6.2488**	**0.0440**	**0.0147**	0.7232	0.4357	$D > C, D \approx S, C \approx S$

D = Digital Assistant, C = Computer, and S = Smartphone.

Table 3.5: Holm-Bonferroni corrected one way Kruskal-Wallis test results comparing for the effect of device type and pairwise comparisons using Dunn tests for themes with statistically significant Kruskal-Wallis test results. Items in bold with blue background are statistically significant.

Not neighbouring, *Reserve with partner*, and *Possessiveness* themes.

3.3.3 RQ2: Effect of *device type*

To understand the effect of device type, we conducted one-way Kruskal-Wallis tests[7] per theme on the means of each participant's responses to the questions in each theme. The Kruskal-Wallis Test results in Table 3.5 reveal statistically significant differences between devices in all privacy themes. We ran pairwise Dunn tests[8] for post hoc testing. Table 3.5 also contains results of the Dunn tests.

For five themes, the Dunn tests revealed that the responses for digital assistants were significantly different from both the computer and smartphone responses. For *Intimacy* and *Anonymity* the digital assistant responses indicate less desire for privacy than the computer and smartphone responses. Conversely, the digital assistant responses indicated greater desire for privacy than the other two groups in the *Not neighbouring*, *Solitude*, and *Reserve with Partner* themes.

The Dunn tests also revealed significant differences between digital assistant and computer responses (but not smartphone responses) for the remaining two themes. In the *Low-self disclosure* and *Possessiveness* theme, the digital assistant responses were

[7]Kruskal-Wallis tests were computing in R using the `kruskal.test` function from stats (version 3.6.2)

[8]Dunn tests were computing in R using the `dunnTest` function from FSA (version 0.9.4)

higher than the computer responses, indicating that participants were less willing to share information or space with a digital assistant than a computer.

3.4 Interpretation of Results

RQ1: ***In which privacy contexts, if any, is social agency attributed to each type of device?*** To answer RQ1, we interpreted the Kendall correlation test results in relation to the privacy theme definitions. The responses for all three device groups indicated social agency in (i) the *Solitude* theme, implying that devices are a distinct agent from the self and that they can intrude when users desire time alone, and (ii) the *Low-self disclosure* theme, implying a similarity between sharing information with a device and with other person.

In the *Anonymity* theme, we found correlations for both the smartphone and computer question groups. This suggests that participants felt similarly about an unfamiliar computer, smartphone, or person knowing about them.

Finally, we found a correlation for the smartphones group in the *Intimacy* theme, which relates to trusting someone – or a device – with sensitive information and forming a privacy social bubble with them. This suggests that participants might formulate expectations about the privacy of their interactions with their smartphone (but not with their computer or digital assistant) similar to their interaction with a close friend.

In conclusion, participants seem to attribute social agency to all three devices in contexts which relate to disclosing information about oneself, i.e., *Low-self disclosure*, and which related to feelings of intrusion when one wants to be alone, i.e., *Solitude*. Participants also attribute social agency to both computers and smartphones in terms of treating devices as distinct entities, *Anonymity*, and to smartphones in terms feeling especially close or trusting towards an actor, *Intimacy*.

RQ2: ***What differences, if any, exist in people's privacy attitudes towards each type of device?*** For RQ2, we are only concerned about the differences between devices. Given the distinctiveness of the digital assistant responses, we interpret each of the themes in relation to digital assistants.

In the *Intimacy* themes, the digital assistant responses were lower than those of the other two groups, which suggests that participants may feel closer to their computers and smartphones than to their digital assistants. *Anonymity* also contained lower digital assistant responses, which suggests that participants are less concerned about an unfamiliar digital assistant knowing their sensitive information than they are to an unfamiliar computer or smartphone.

The *Not neighbouring* responses were higher for the digital assistants than for the computers or smartphones which again indicates greater desire for privacy from a digital assistant than a computer or smartphone. Furthermore, the digital assistant responses were higher than those for computers or smartphones in the *Solitude* theme which points to participant's desire to have more time away from their digital assistants than from their computers or smartphones. The same trend occurred in the *Reserve with Partner* theme, suggesting that participants are more reserved with their personal digital assistants than with computers or smartphones.

The digital assistant responses indicated higher desire for *Low-self disclosure* and *Possessiveness* than their responses to computer questions. This suggests that participants are less likely to want to share information, items, or space with their digital assistant compared to their computer.

Overall, responses tend to indicate that participants desire greater privacy from digital assistants than they desire from smartphones and computers. They are less likely to include digital assistants in their private social bubbles, and seem to find digital assistants to be more intrusive when looking for time alone. Responses to questions about digital assistant were most different from response about computer; users were less likely to feel comfortable sharing information or space with their digital assistant than their computer. However, digital assistant responses indicated less desire for privacy compared to responses to questions about computer or smartphone for the *Anonymity* theme. Perhaps users find it less objectionable for a digital assistant to know information about the users given that a key part of digital assistants' functionality is seamless interactions across different physical devices.

In conclusion, there were two key differences in the CASA-related privacy attitudes expressed towards the three devices. Responses indicate that participants desire

greater privacy from digital assistants than the other devices. Also, participants desired less anonymity from digital assistants than from computers and smartphones.

3.5 Limitations

First, we used only a subset of the themes from the psychology privacy preference scale papers due to the necessity of having matched person and device questions and wanting to reduce the demand on our participants' time. We pilot tested our survey to ensure that the questions seemed reasonable in both the person and device phrasings. Despite these efforts, we needed to eliminate several of our questions during factor analysis. In the future, it might be worth building a purpose-built privacy attitude scale with matched person and device questions.

Secondly, we thought it was important to use a within-subjects design so that we could directly compare a participant's device and person responses. Though we ensured that participants were not presented with matched person and device questions sequentially, some participants could have recognized the matched questions which may have primed their responses.

Thirdly, the survey is testing for two things: perceived social agency and privacy preferences. It is possible that a participant's privacy attitudes towards another person or a device interferes with whether their responses indicate that they treat their device as a social actor.

Finally, by recruiting through Prolific, our sample reflects individuals who are reasonably comfortable with technology and the median age of our participants is 32 years of age (Table 3.4), so our results reflect a younger demographic who may have different relationships with their devices.

3.6 Conclusion

We conducted a survey based on psychology privacy preference scales to explore the possible relevance of the CASA paradigm to privacy contexts for computers, smartphones, and digital assistants. Our results indicate that participants apply human-human interaction scripts to their interactions with devices in four privacy

themes: *Intimacy*, *Solitude*, *Anonymity*, and *Low-self disclosure*. Moreover, we found no significant differences between the responses to questions about computers and smartphones, but responses for digital assistants were most often significantly different from both computers and smartphones. Our findings suggest that users are more comfortable sharing space and sensitive information with computers or smartphones compared to digital assistants.

Chapter 4

Interview Study

Our questionnaire results provide some evidence that there are instances when participants' privacy interactions follow human-human interaction scripts. However, a questionnaire fails to capture the nuances of how participants' privacy attitudes and behaviours might be affected when following human-human interaction scripts. We also wanted to create a theory which could explain how CASA influences people's privacy attitudes and behaviours. Such a theory would address our third research question, RQ3: *How, if at all, are people's privacy attitudes explained by CASA?*. Therefore, we conducted semi-structured interviews following a grounded theory methodology.

4.1 Methodology

Carleton University's Research Ethics Board provided clearance for the study.

4.1.1 Grounded Theory Methods

We followed Charmaz's methodology from *Constructing Grounded Theory* [20] for this study. Grounded theory derives its name from the fact that it is a methodology where you seek to develop a theory that is grounded in the data. Charmaz describes grounded theory as a set of "systematic, yet flexible guidelines for collecting and analyzing qualitative data to construct theories from the data themselves" [20]. During grounded theory studies, we follow a cycle of continuously collecting and analysing interview data. Charmaz argues that this methodology allows researchers to modify their interview guides based on previously collected and analysed data and encourages them to pursue ideas and concepts related to the research goal, but were not explicitly included in the interview guide.

Given the lack of research connecting CASA directly to privacy attitudes and behaviours, we felt it most appropriate to employ grounded theory since it is well

suited for exploring topics with limited existing research. Moreover, we felt that developing a theory about the CASA's relationship to privacy would help to anchor a research agenda which could connect the previous literature which is adjacent to CASA but does not explicitly connect to it. A theory could also act as a foundation for CASA privacy design principles to help guide privacy design.

The interview sessions were semi-structured and the interview guide evolved as we completed and analysed interviews, so all participants were not necessarily asked the same questions. Section 4.2.4 provides greater detail on how we updated the interview guide.

4.1.2 Study Overview

The study unfolded according to the following steps:

1. We released the pre-screening survey to batches (5-15) of participants on Prolific.

2. We contacted eligible participants to organize the interview.

3. We conducted interviews with consenting participants.

4. After each interview, we transcribed the interviews and performed initial coding.

5. We modified the interview guide by adding or changing questions so that we could pursue emergent themes or fill gaps in the data as they appear in the analysis.

6. We repeated steps 2-5, screening, interviewing and coding transcripts in batches, until we reached saturation for the theme as intended in the study guide.

4.1.3 Recruitment

We recruited participants in March and April 2023. Participants needed to be over the age of 18, currently reside in Canada, and be able to complete an interview in English. They also needed to use at least two of the following devices: computer, smartphone, or digital assistant (e.g Google Home, Amazon Echo, etc). Interested

Demographic	Number of Participants
Province of Residence	
Alberta	4
British Columbia	5
Manitoba	1
New Brunswick	2
Ontario	15
Quebec	1
Saskatchewan	2
Gender	
Women	18
Men	12
Self-Described Tech Experience	
Yes	9
No	21
Median Trust Score (out of 5)	3.8
Median Age (in years)	33
Median Survey Completion Time (in seconds)	94

Table 4.1: Demographic information for pre-screener participants

participants completed a pre-screener using the UK-based crowd-sourcing platform Prolific[1]. Based on Prolific's suggested payment rates, we paid participants 0.45 GBP (approx. 0.75 CAD) upon completion of the pre-screener. Upon completion of an interview, we paid the participant an additional 12.50 GBP (approx. 20.00 CAD).

4.1.4 Pre-Screener

On Prolific, we used a pre-screener survey to recruit participants. Firstly, we asked participants some basic demographic questions. We asked participants to select their gender, provide their age, and the province in which they currently reside. We also asked if they had any had experience in computer science, information technology, or a related field. Then we asked participants which devices they used (computer, smartphone, or digital assistant) and how frequently they used each of their devices. Finally, we asked participants questions to identify their general trust attitudes so that we could try to obtain a participant sample including diverse attitudes about

[1] `https://www.prolific.co/`

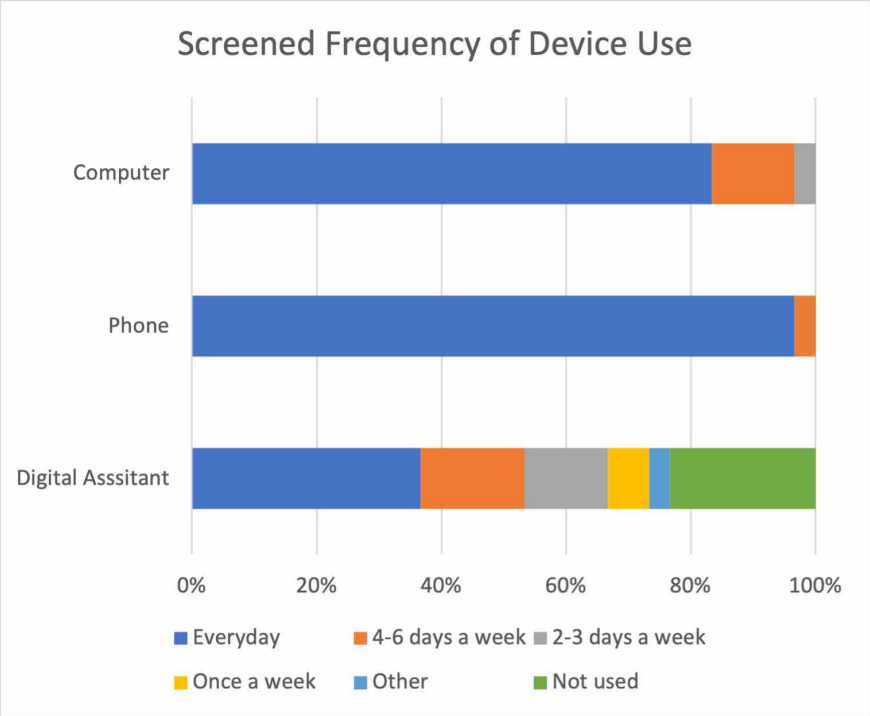

Figure 4.1: Screened participants' self reported usage of their devices (including interview participants).

trust. We used Yamagishi and Yamagishi's General Trust Scale [89] which uses six five-point Likert-questions to obtain a high-level understanding or respondents' trust attitudes. A participant's trust score is the average of their responses to the six five-point Likert-questions (we report the median score of the screened participants in table 4.1. The set of the questions asked in the pre-screener survey is available in Appendix B. We used the participants responses to the pre-screener to invite a diverse group of interview participants.

The pre-screener survey had a median completion time of approximately 1 minute and 34 seconds. We compensated participants 0.45 GBP for participating. A breakdown of the respondents' demographics is available in Table 4.1, and device usage in Figure 4.1.

4.1.5 Interview Participants

ID	Age	Gender	Tech	Trust Score	Computer Use	Phone Use	Digital Assistant Use
P1	22	Man	Yes	3.33	Everyday	Everyday	Not used
P2	35	Woman	No	4.33	4-6 days/week	Everyday	2-3 days/week
P3	39	Man	Yes	3.67	Everyday	Everyday	Not used[2]
P4	36	Woman	No	3.83	Everyday	Everyday	Everyday
P5	66	Woman	No	4.17	Everyday	Everyday	Everyday
P6	21	Man	Yes	2.00	Everyday	Everyday	4-6 days/week
P7	30	Woman	No	3.50	Everyday	Everyday	Everyday
P8	37	Man	No	3.83	Everyday	Everyday	2-3 days/week
P9	41	Woman	No	4.17	Everyday	Everyday	Everyday
P10	36	Woman	Yes	4.17	Everyday	Everyday	Not used
P11	38	Woman	Yes	4.00	Everyday	Everyday	Everyday
P12	29	Woman	No	3.17	Everyday	Everyday	Once a week

Table 4.2: Demographic information for interview participants including participants' self reported device usage in the pre-screener. The "Tech" column represents whether participants self-described as a technology expert.

We selected participants from among those eligible and contacted them via Prolific's internal messaging system to schedule an interview. We used the results of the screening survey to try and achieve diversity across participants self-described demographics, device usage, and trust. If several participants in a batch of pre-screener responses were eligible, we prioritized participants with gender identities, ages, provinces of residence, or trust scores which were underrepresented in our sample.

In the end, we interviewed 12 participants. Demographics and self-described device usage for the interview participants are included in Table 4.2.

4.1.6 Interviews

We interviewed participants remotely over Zoom[3] for approximately 45 minutes each. We compensated participants 12.50 GBP for their time using Prolific's bonus payment system. We recorded every interview with Zoom's built-in system for recording meetings. We transcribed each interview immediately after it concluded using the

[2]In the pre-screener, P3 explained that he stopped using their standalone digital assistant but still use the digital assistant on their smartwatch.

[3]`https://zoom.us/`

transcription software Trint[4]. Once transcribed, we removed all copies of the interview recording from Trint and the primary researcher's computer.

The interviews were semi-structured and the interviewer tailored the questions in each to best address the attitudes and experiences of the participants. Generally, the interviewer asked them questions about their experiences with the devices (computers, smartphones, digital assistants) they had used. During the interview, the interviewer made notes on their computer to keep track of ideas and topics so they could ask follow-up questions.

4.2 Analysis

In keeping with our interview approach, we followed Chamaz's recommendations for developing a theory grounded in the interview data. We detail our analysis process below.

4.2.1 Researcher Background

All analysis was performed by the primary researcher, Maxwell Keleher, who had also completed all of the interviews. He is a Human-Computer interaction master's student with a background in Computer Science and work experience as a Software Engineer. He also has experience in studying technology from a media and cultural studies perspective. He subscribes to the outlook that technology is not culturally or morally neutral and recognize that all work done to interrogate technology must be filtered through the author's perspective and past experiences. As a result of his mix of experience in computer science and humanities, he greatly values interdisciplinary approaches to studying and discussing technology. This is his first time employing grounded theory methods. The original purpose of this interview was to understand how CASA affects participants' privacy attitudes and behaviours, however, he remained open to adjusting the direction the study based on the content of the interviews.

[4] `https://trint.com/`

4.2.2 Coding

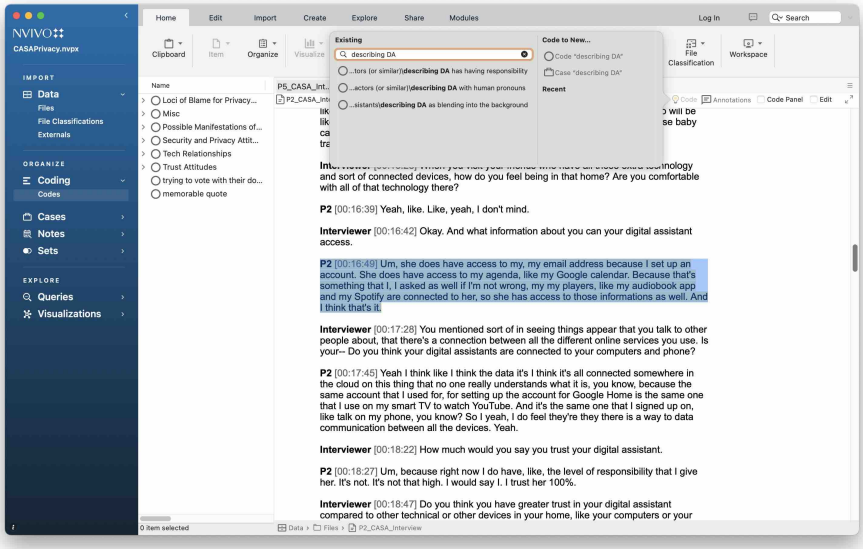

Figure 4.2: Example of how open codes were applied to paragraphs by paragraph in NVivo.

Some higher level codes and themes were noted in the memo book after the interviews, while transcribing the recordings, and when performing the initial coding. For the coding process, the transcripts were imported into NVivo where we performed paragraph-by-paragraph open coding (see Figure 4.2). We did not apply pre-existing codes or themes but rather followed Charmaz' recommended gerund based approach which highlights participants' actions and experiences. Every two to three interviews, we used focus coding to search for patterns in the responses between participants. This allowed me to develop rough categories and themes which were later refined through sorting.

After 8 interviews, we performed axial coding to sort the focused codes into high-level categories and themes which would later form the basis of the final theory. Once we had open coded the final interviews, we used an affinity diagram to assist with the final axial coding process and generate the theory. We detail the theoretical sorting and theory generation process below.

4.2.3 Memos

As suggested by Chamaz, we kept a memo journal to make notes during interviews as a space to make observations and theorize throughout the research process. During the interviews, we used the memo journal to note possible code categories and themes. While sorting, we made notes to brainstorm the final theory. Overall, we opted to work through most of the theory development visually through the affinity diagram and model of the actors considered in participants' privacy attitudes. In the end, we had about five letter pages of notes.

4.2.4 Updating the Interview Guide

There were minimal changes to the interview guide because the initial version broad enough to get participants to bring up their own experiences which we could probe. Generally, we focused on trying to probe into moments where participants described treating their devices as social actors or where they mentioned actors other than the device. For example, we added the question *Why did you choose that brand of device?* when participants explicitly mentioned the brand of their devices. To avoid priming participants to mention specific actors, we did not add other questions about the specific actors and rather probed about the actors or scenarios participants brought up naturally in the interviews.

4.2.5 Theoretical Sorting, Diagramming, and Integrating

Within NVivo, we sorted codes into five main categories identified through focused and axial coding: (i) loci of blame for privacy violation, (ii) social and emotional responses to technology, (iii) security and privacy attitudes, (iv) relationships with technology and tech actors, (v) trust attitudes. See Figure 4.3 for how codes were categorized in NVivo. Within these categories, we grouped the codes into subcategories based on which of the three devices they were referring to. As an example, within the tech relationships category, we had subcategories for each of the three devices. In some cases we added subcategories to collect codes which addressed a common actor (a human, device, or entity with whom a participant interacts) or topic. For example, we moved the category about relationships and opinions regarding brands

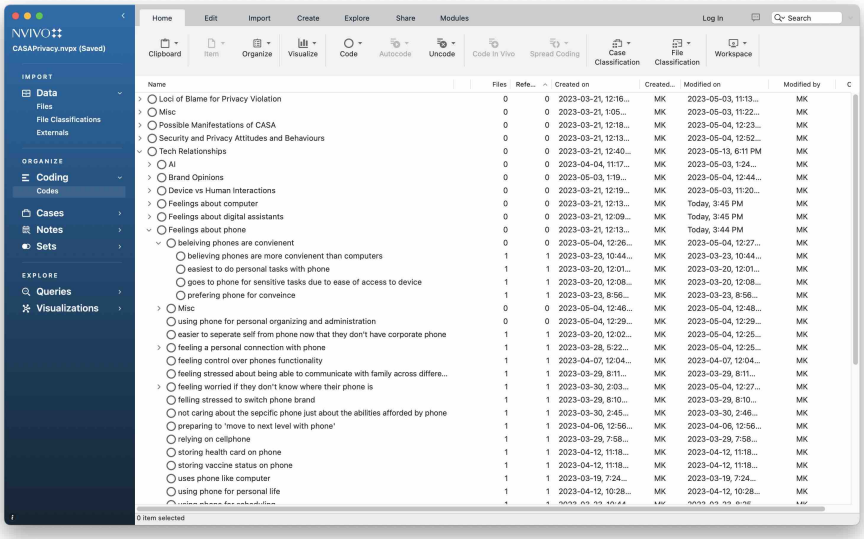

Figure 4.3: Example of how we grouped codes into categories in NVivo.

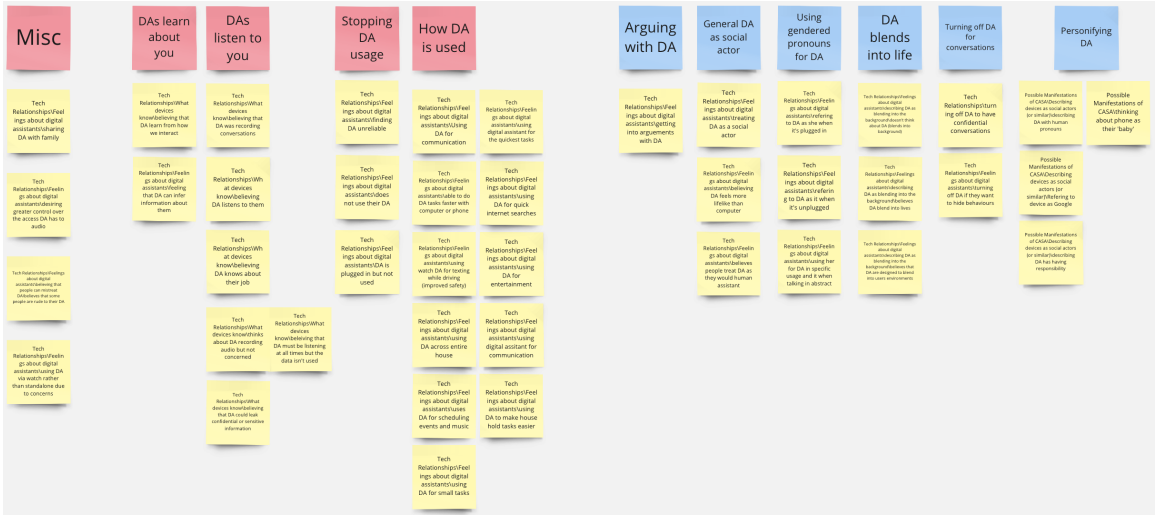

Figure 4.4: Example of how we sorted codes in Miro for Digital Assistants. We used pink to identify top-level codes about device usage and blue to identify top-level codes related to CASA.

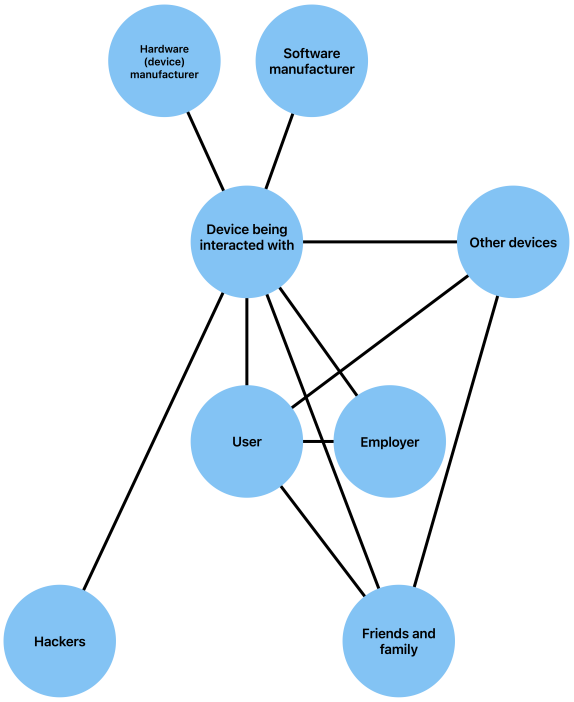

Figure 4.5: Initial draft of the diagram for understanding how participants considered actors other than computers, smartphones, and digital assistants in their privacy attitudes and behaviours towards the devices.

into category (iv) – which held all the codes pertaining participants' perceptions of actors associated with technology.

After completing the final phase of axial coding in NVivo, we exported the codes to Miro for affinity diagramming. At first, we worked on diagramming per category but when a common theme emerged we began to build thematically related collections out of groups of codes. As the common actors emerged, we moved relevant codes from the five main categories into subcategories – or new, top-level categories – based on the actor to which they related. For example, Figure 4.4 shows that we organized attitudes towards the three devices. We followed a similar strategy to understand attitudes and behaviours related to other common actors. As the different actors became apparent during the sorting process, we began to develop a diagram to represent our final theory.

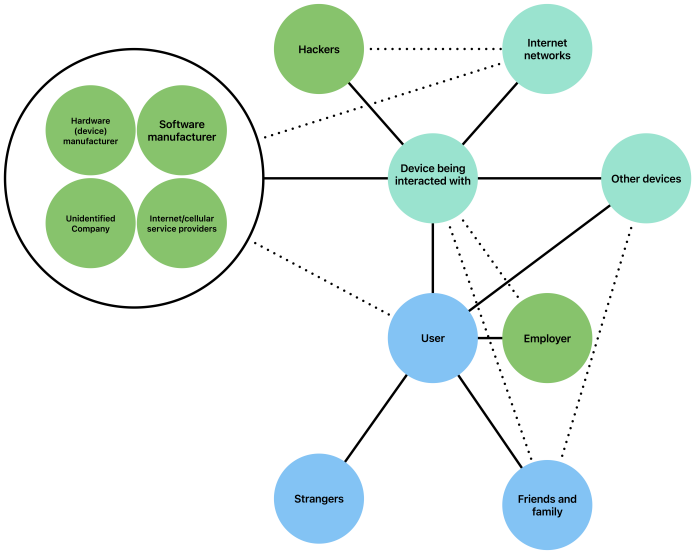

Figure 4.6: Iteration on the theory diagram. In this diagram we differentiate between different groups of actors (blue for human actors, teal for device actors, and green for companies) and identify common and uncommon interaction (indicated by solid and dotted lines respectively)

4.2.6 Theory Construction

As we grouped codes about participants attitudes towards and behaviours with their devices, we pulled out codes which seemed to indicate perceived social agency of their device. It became clear that in their privacy attitudes and behaviours, participants considered actors other then just the devices with which they are interacting. We broke down our existing categories and recombined codes to build out groupings which described how participants considered the different actors when describing privacy attitudes. Other than the device which they were interacting with, participants seemed to consider other devices they owned, other humans, and corporation in their privacy attitudes and behaviours. We visually represented the multitude of actors participants considered in Figure 4.5 as a means of organizing our thoughts around the theory.

In Figure 4.6, we iterated on our initial diagram by trying to organize the actors. We grouped the companies since most connected to the other actors in the diagram in the same way and colour coded related actors. Blue represented human actors with whom the participant directly interacts. Green were humans with whom the

participant might indirectly act or were more abstract social groups. Teal indicated devices or other pieces of technology. We also distinguished between two types of interactions: solid lines represent interactions between the two actors which very frequently mentioned by participants, whereas dotted lines indicate interactions that only a few participants seem to consider.

Through consultations between the primary researcher and the supervisor, we simplified the diagram once more (see Figure 4.7) by focusing on actors which were explicitly connected to privacy topics. Moreover, actors in the final diagram should be related to how the participant interacts with a particular device rather than someone or something considered in the abstract. We chose more distinct colours and shapes to distinguish between the different actor groups as well as changing the shape. Now blue triangles represents humans actors, purple circles represent device actors, and green squares represent corporations or brands. Due to the limited sample size of our interviews, we also opted not to distinguish between possible and definite connections between actors.

This simplified diagram also re-emphasized the interaction between the participant and a particular device, and provides an opportunity to highlight the ways that CASA informed and influenced participants' attitudes and behaviours with their computers, smartphone or digital assistants.

Next, we lay out evidence supporting the construction of the different components of the theory. We articulate the full theory in light of the study results and discuss how the different components of the theory relate to each other in Section 4.5.

4.3 Results

In our interviews, we found several instances where participants' privacy attitudes appeared to be impacted by CASA. When describing their smartphones and digital assistants, participants sometimes applied human-human scripts when discussing their privacy attitudes and behaviours. Notably, we found that attitudes and behaviours were not based solely on the interaction with and perception of a given device. Rather, participants seem to consider a group of related actors which include other humans, other devices, and corporations (see Figure 4.7).

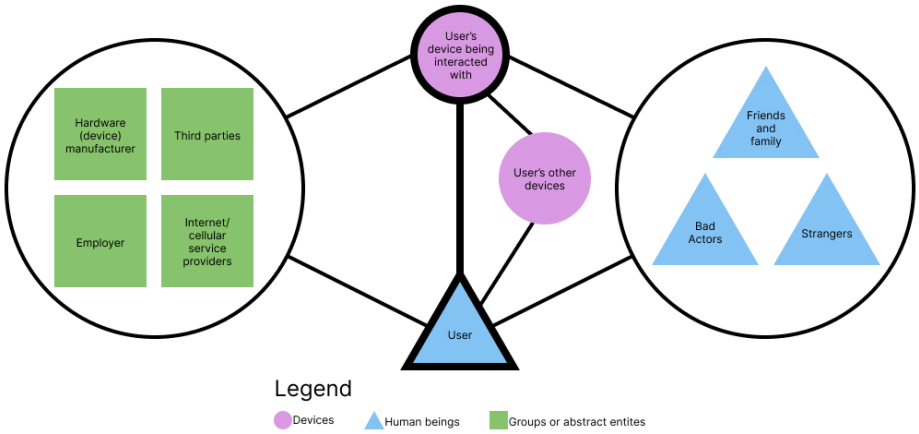

Figure 4.7: Final diagram showing which actors participants consider in their privacy attitudes and behaviours. We improved differentiation of actor groups by using more distinct colours and changing the shapes.

While our stated research question, *How, if at all, are people's privacy attitudes explained by CASA?*, only references the interaction between the participants and the device, we feel that it is important to portray the wider scope of actors that participants discussed in our interviews. Therefore, we propose two components to our theory:

1. CASA can explain participants' level of comfort or discomfort sharing private space or information with their devices,

2. In their privacy attitudes and behaviours, participants consider multiple actors beyond just the device with which they are interacting.

In the remainder of the results, we explain how participants described each of the actors identified in Figure 4.7. First, we address the first component of our theory, by describing how CASA relates to participants' privacy attitudes and behaviours. We cover the attitudes and behaviours participants described towards each of the three devices, focusing on attitudes and behaviours which relate to CASA. Then, we provide evidence supporting the second component of the theory; We explain the ways that participants considered additional actors (i.e., other devices, other humans, and companies or brands) in their privacy attitudes and behaviours towards computers, smartphones, or digital assistants.

4.3.1 Interactions between participant and main device

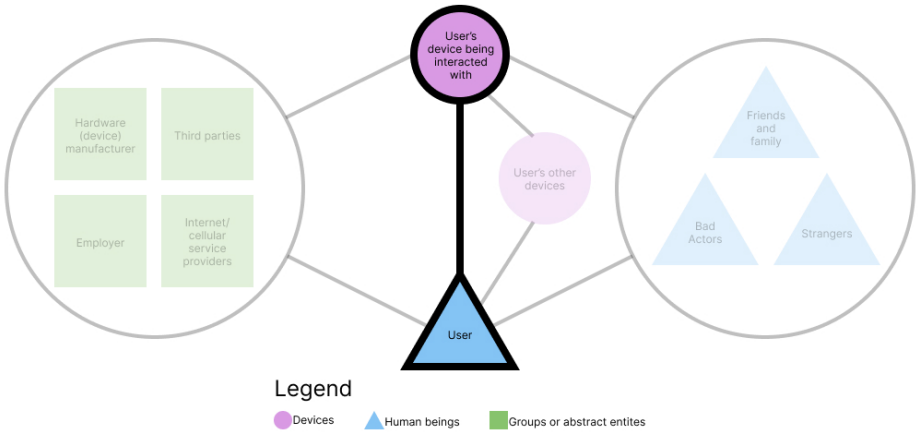

Figure 4.8: Diagram highlighting the interaction between a participant and their smartphone, digital assistant, or computer.

In this section, we explain our theory of how CASA relates to participants' privacy attitudes and behaviours in their interactions with smartphones, digital assistants, and computers (visualized in Figure 4.8).

We found evidence of CASA during the interviews. Participants appeared to attribute social agency to their devices, and some participants even discussed their devices in terms of "he" or "she", or about their device "knowing" things about them. With respect to privacy, two main possibilities exist: that CASA leads to comfort with information disclosure or that CASA instead leads to feelings of intrusion or mistrust. We found evidence of both. While these two attitudes are contradictory, the connecting thread is that each occurred in relation to participants' perception of their device as a social actor. Therefore, We theorize that there is a relationship between perceiving a device as a social actor and feeling comfortable disclosing sensitive information to the device. There seems to be a cyclical relationship wherein (i) perception of social agency drives comfort disclosing information and (ii) sharing space with a device and comfort with the device drives social agency (see figure 4.9). Conversely, there is also a relationship between perception of a device as a social actor and feeling that the device intrudes into personal space. Similar to above, there appears to be a cyclical relationship between perceiving a device as a social actor and feeling that the device is intrusive (again see figure 4.9).

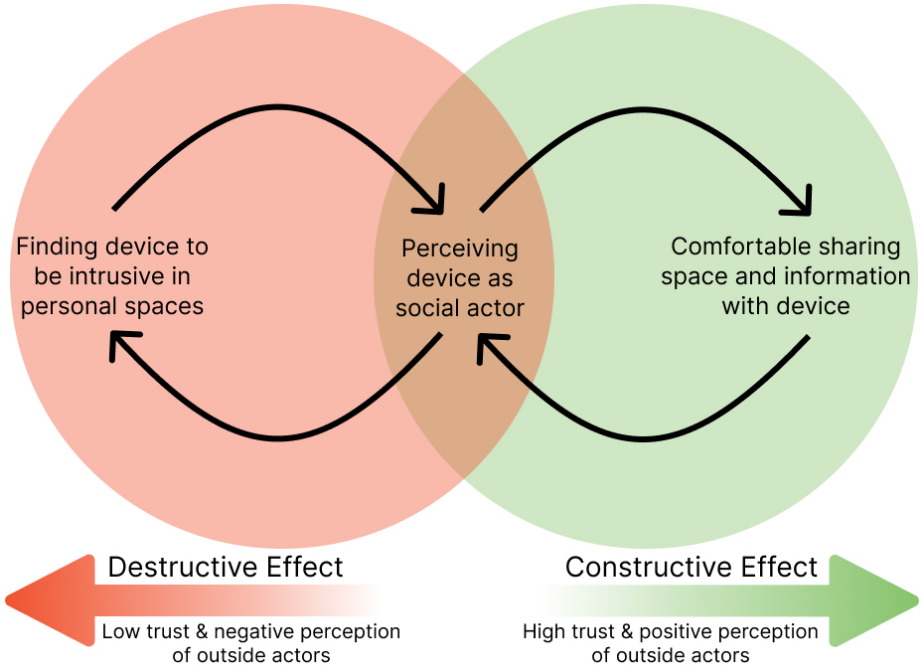

Figure 4.9: Diagram of the relationships between privacy attitudes and behaviours for devices and perception of devices as social actors.

Therefore, CASA can have a positive effect on a user's comfort with devices (*constructive effect*) or a negative one (*destructive effect*). Whether the effect will be constructive or destructive depends on contributing factors such as participants' general trust and privacy attitudes, and, effect of outside actors such as other humans, other devices, and related companies. We provide more explanation regarding the effect of outside actors, which is the second component of our theory, starting in Sections 4.3.2, 4.3.3, and 4.3.4. Below, we highlight the CASA-related privacy attitudes participants expressed towards their smartphones, digital assistants and computers.

Smartphone

Participants seemed to view their smartphone as a device with which they had an especially close relationships. Participants expressed that they were comfortable with their smartphone having access to sensitive information such as their credit cards. When we asked why they were especially comfortable sharing with their smartphone, participants referenced closeness, both physical and perceived, as the reason. P10

explained:

> I have my phone on me at all times, I know what I do on my phone. I don't have access... Like, my phone is my phone. I'm the only one that touches my phone. Whereas the computer. I have other people that touch the computer. (P10)

P8 had described how his smartphone was an incredibly important part of his life and used the following story to highlight this importance:

> Before we had kids [my wife and I] would look at our phones as our babies. [...] Now we have children, so I worry about them instead of my phone so much. (P8)

P9 also used language that alluded to a close relationships similar to that used with friends or family. She described that she was "ready to jump to the next level" with her smartphone by connecting it to a wearable device "allowing [her] smartphone to maybe help support [her] in some of these lifestyle choices that [she's] making". Her comfort with revealing personal health and location data seemed to correspond with a feeling that she already had a comfortable relationship with her smartphone and felt that it could provide some support to her goals. Due to perceived closeness, participants seem more likely to be comfortable with sharing sensitive information with their smartphone.

Some participants described their smartphones as being some sort of extension of themselves. P5 and P8 both referenced feeling "naked" when they did not have their smartphones. P8 described a greater sense of feeling incomplete without their smartphone:

> It sounds crazy, but I kind of feel, like I'm gonna say, incomplete without my phone. [...] I live in a situation now where I have more ability than my own actual body can do right now. Like my actual body can lift things and throw things and run and talk and think. But I can also access information with my phone and I can communicate to other people in the world. (P8)

These descriptions of participants' relationships with the smartphone might echo the way that some people might refer to their partner as their other half or as completing them in some way.

Participants' descriptions of how they interact with their smartphone seem to indicate they perceive their interactions with their smartphone to be the most confidential of the three devices. P9 explained how she and her partner see their smartphones as being especially private devices:

> I just feel like I just want one thing that's private. So, like, my partner is pretty private with his phone, and I don't ask to look at it. And I'm pretty private with my phone, so we don't really, you know, interfere with each other's phones. (P9)

When describing her relationship with her smartphone, her language seemed to evoke a human relationship with a trusted companion.

> Gosh, I probably accidentally sleep on top of my phone without even realizing it. [...] I don't have like a Fitbit, but I mean, I think the only thing my phone probably doesn't know about me is my heartbeat. But it [...] knows my steps. [...] It knows what route me and the dogs will take to the park. It knows like what time I take my medication because I have an app that reminds me. Like, yeah, basically everything. I would imagine probably knows when I'm like having a bad day. Notice when I, you know, I'm staying up too late. (P9)

For participants, smartphones seem to be perceived as sitting somewhere between social actors and extensions of the participants' own body. Consequently, participants seem much more comfortable allowing smartphones to access and track sensitive information.

Digital Assistant

During interviews, many participants explicitly personified their digital assistants: some gendering their digital assistant and/or describing how they treat it as they

would a human assistant. P5 explained that she often gets into arguments with her digital assistant:

> I get into arguments with her, basically, because I'll ask her something, which I think, you know, she should be able to dig out of her, you know, voluminous memory banks. But she sort of goes like, 'yeah, no, I don't really care'. And I go, you know, 'that's what you're supposed to be doing'. [...] Then I tell her to stop listening and shut down, [...] sort of putting her on a time out. So she's quite real to me. (P5)

Later P5 unplugged her digital assistants after if had been unintentionally activated and noted:

> You noticed when she's, when she's not plugged in, I referred to her as an it. When she's plugged in, I refer to her by her name. And it's like right now she's just [...] sitting there. [...] It's just [...] an appliance. But when she's plugged in, I think of her as a person mostly. (P5)

P5 was not the only participant who gendered her digital assistant. P4, who mentioned owning an Amazon Alexa, explained that she and her family "use her to set a timer for everything". When asked if she trusted her digital assistant, P2 stated, "I trust her 100%" because she does not "give her [digital assistant]" a high "level of responsibility" and therefore there are few ways that the digital assistant can invade her privacy.

Other instances of participants treating their digital assistants as social actors occurred when some participants felt digital assistants could be mistreated. P2 described how she thought it was inappropriate to get "mad" at your digital assistant and tell it to "shut up" since it may "remember" that you were rude. P9 also mentioned that she will sometimes "argue" with her digital assistant and feels that people generally need to be "polite" to digital assistants because people "teach" their digital assistants how to behave. She went on to tell a story about how her digital assistant will "respond differently" based on how it is treated:

> [My partner and I] were eating dinner and I said, 'Google volume will lower' and then Google responded to me and said, 'in order to turn the

> volume lower, just say lower or higher.' And then I said, 'okay, lower'. And then it wasn't working. And then [my partner] said, Google lower. And then his Google was like, 'I don't understand that command' [...] I kind of got the sense Google was just messing with me because we were just kind of yelling at it. (P9)

There was also a feeling for some participants that their digital assistants could invade their privacy. Some participants felt that their digital assistant listens to them even when they would not wish for it to. P1 said:

> [I] considered whether it records audio, but I think it's doubtful but not too sure about that. (P1)

P8 expressed that they feel their digital assistant must be "listening at all times" since they receive advertisements about things they talk about around their home. Some participants were more put off by the sensation of being listened to: P3 felt much more invaded by his device when he and his wife noticed it "listening" to them:

> You know, when you watch a horror film and something drastic happens and there's a moment of silence and then there's a moment followed by when you look at each other and you're like, 'What just happened?' So we were startled initially, and then we started to realize that, you know, as life becomes more digitized and digital and accessible, there are pros and cons of it, right? [...] That's really the feeling and reaction to it. It was a little scary. (P3)

Fascinatingly, one of the participants described how she would use her "native language" when she is discussing sensitive information with her family, such as banking information, and she doesn't want her "voice to get captured". P11 explained that her native language sometimes feels like a "secret code" so that "people around [her] don't listen" when she needs to communicate sensitive information.

Unlike smartphones, it seems that for some people, CASA can inspire negative attitudes towards their devices with respect to privacy. None the less, some participants still seem to feel comfortable sharing space and information with their digital assistants because they treat them as they would a human.

Computer

Participants' privacy attitudes and behaviours related to computers seemed to be least impacted by CASA. Unlike smartphones and digital assistants, participants did not describe their computers with the same personifying language. P1 stated that his computer is a "tool for [his] work". P5 said that she considers computers to be "just a device" and that she does not feel "empathy" with them.

The other unique aspect of discussions about computers is that participants desired having devices which were dedicated to particular tasks. P6 said that his "ideal scenario" was having "another computer altogether" that could be dedicated to "banking" or "taxes". Similarly, P3 said that he has a dedicated laptop for travelling because it would be a "big problem" if the "trading information" on his personal laptop fell into the wrong hands. He went on to explain that he prefers to keep "different pockets of [his] life in a different sphere".

Other participants mentioned that they dedicate their personal and professional computers to personal and profession tasks. P1 said that he wishes to keep his personal and professional stuff "separate" and that he tries to "strictly just do work stuff" on his personal laptop. P3 talked about his interest in trading stocks, but explained that since he works as a public servant, he only looks at stocks and market information on his personal laptop so that these personal and professional lives don't "intersect in a negative way". Similarly, P2 said that she doesn't "use my work computer [to participate in Prolific studies] or watching, like, YouTube or whatever". Overall, participants' privacy attitudes and behaviours towards computers seem less obviously affected by CASA than those towards smartphones and digital assistants.

4.3.2 Other Humans

The second component of our theory is that: participants' relationships with the additional actors (i.e., other devices, other humans, or companies) could cause participants to feel more or less comfortable sharing information or personal space with the primary device (see Figure 4.10). Generally, positive relationships with the additional actors had a positive effect on comfort, and negative feelings towards the

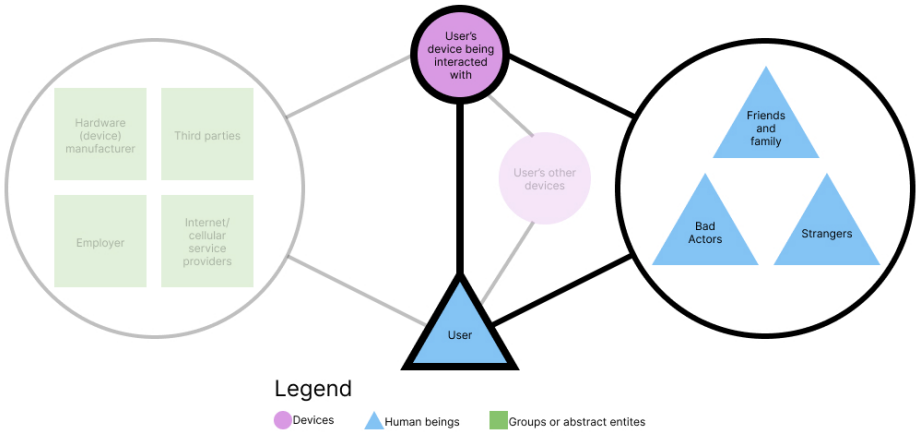

Figure 4.10: Diagram highlighting how participants consider other humans – family, bad actors, and strangers, in their interactions with their devices.

additional actors had a negative effect on comfort. In the following sections, we explain how participants considered other humans, other devices, and corporations in their privacy attitudes towards their devices.

Some privacy attitudes or behaviours related to sharing information or data with their devices were in fact based on their consideration of other humans. Participants mentioned 3 main groups of humans during interviews: friends and family, bad actors, and strangers.

Family

Participants considered friends and family in their privacy attitudes in 3 different ways. Firstly, some participants were comfortable sharing their devices with their family. P4 described how her husband has "full access" to her smartphone since she "shares her passwords with him [...] even with FaceID, there's a passcode to get into the smartphone so he knows it" (P4). Similarly, P8 explained his decision to have several digital assistants within his house by explaining how it benefits his family and their ability to communicate:

> We have maybe three or four [digital assistants] Three of them downstairs and my mother in law has one upstairs [...] We use them to communicate back and forth, which is good. You know, the broadcast feature which which is helpful, if you can call the kids up to come get something. (P8)

Secondly, there were participants who specifically saw their devices as enabling their family to invade their privacy. P9 would sometimes turn off the camera on her digital assistant because she knew that her "partner can see the camera" and she does not always want him to "see what [she's] doing". She also avoided sharing text messages between her smartphone and computer since her husband "could look at, like, every single text message"; even though she doesn't "have anything to hide" there is a "certain level of privacy that [she and her husband] just both allow for each other". Critically, it would seem that devices can be invasive in and of themselves but they can also be a means by which other people might invade your privacy. So in privacy, it might be that devices are not *always* social actors. P11 explained how she saw some devices as threats to her family's privacy and would therefore try to take steps to protect her family. When asked about digital assistants and privacy, P11 expressed concern about whether her devices might be surreptitiously listening to her family and may be recording a "very private moment between your family and you or between your spouse and you". P11 explained that she has not connected her smart doorbell to her TV since she worries it might "scare [my] children". P11 considered how possible privacy invasions might affect not just herself but also her family.

Other participants also considered effects on their family but they thought that certain features that impacted privacy had positive uses. P4 said that location tracking from smartphones gives her "peace of mind" and is a "security blanket" since she and her husband can see "exactly where each other are" if they can't reach each other and are worried about each others' safety. P9 described how he was able to keep an eye on his elderly parents since they also use iPhones: "[when I'm] worried where my parents are, I can just literally go onto my phone and say, you know, my parents are here". In these cases, ostensibly privacy invasive aspects of devices were in fact desired by some participants to afford feelings of safety about their family.

Overall, participants' privacy attitudes and behaviours were not driven exclusively by self interest. Participants also considered their family members as actors who can either be affected by the participants' privacy decisions or be possible invaders of the participants' privacy.

Bad Actors

Some participants brought up explicitly bad actors who might purposely seek to harm others when describing their privacy attitudes towards their devices. Participants' perceptions of bad actors in the physical world seemed to drive them to store their sensitive information digitally on their device.

P8, who did not indicate that he had experienced being hacked or that his privacy had been violated, seemed to feel safe with respect to attackers since he thought that misuse of user data is rare and would require "a bad faith actor in order to do it. Somebody, you know, somebody who has access to the data, who is doing something that they they shouldn't be doing with it" (P8). It might be the case that participants who did not experience privacy violations in the past would not consider bad actors to be a tangible threat.

Generally, bad actors appeared in participants' descriptions or justifications of privacy attitudes much less frequently than we initially expected. However, some some still remarked how their awareness that there are people who may wish to maliciously access or distribute their sensitive information influenced how they used their devices.

Strangers

Generally, participants' perceptions of strangers came up while discussing their comfort sharing sensitive information with their devices. P12 justified her comfort sharing sensitive information with her devices by explaining that she is more concerned about privacy invasion from people she encounters face-to-face. She feels like an "average person" would not be able to access her information so she feels that her sensitive information on her devices is safe from "people that I might see on the street" and "the creepy guy that doesn't leave [her] alone". Similarly, P1 seemed to believe that he could avoid privacy violations from strangers by using his device to complete tasks. P1 expressed concern that when calling his bank, "the thought crosses [his] mind where like a person I'm speaking to just like now has the my credit card number, the PIN and the expiry date" and that the person on the other end is "just an employee of like whatever businesses, and they could write it down and then go and use it in

10 minutes". P1 felt much more comfortable banking with a smartphone app since he "[doesn't] really think [there's] a person there watching [him] type [his bank information] in". These participants seem to consider their interactions with their devices to be more private than their interactions with other people.

Furthermore, other participants see strangers as a threat to the privacy of their interaction with their devices such as P11 who recognizes that her devices are physically vulnerable. P11 worried about "theft and loss" of her smartphone, since, during the "journey of the phone being lost and found" if someone "found [her] information to give it back to [her]" she would need trust it was in "safe hands". She also explained that she had previously bought a used device and found that the previous owners "didn't even do a wipe of [the device]" before selling it. She wiped the device and alerted the seller and wondered "will everybody do it?" She fears other people are not as "tech savy" and may not think to remove sensitive information before selling.

4.3.3 Other Devices

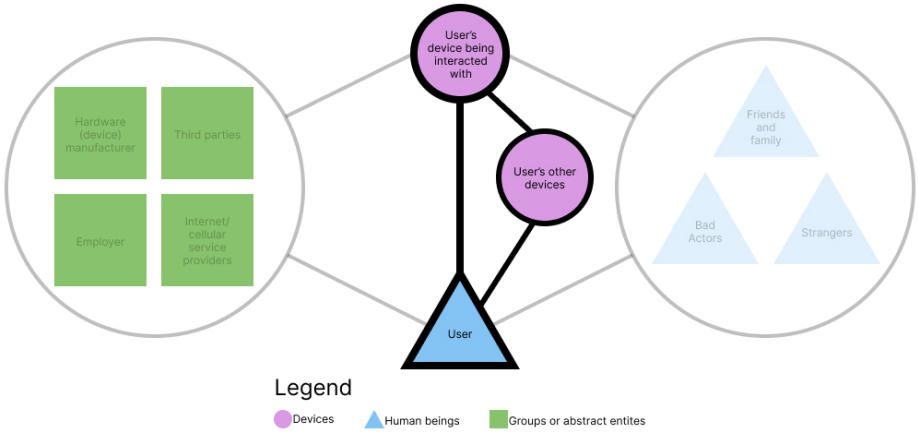

Figure 4.11: Diagram highlighting how participants consider devices other than the one with which they are interacting in their privacy attitudes and behaviours

In conversations with participants, several privacy attitudes or behaviours were, upon probing, revealed to be based upon considerations of devices beyond the device with which they were directly interacting (see Figure 4.11). Some participants felt that their information was shared across several different devices and was not kept confidential to the devices they were interacting with. P6 described that he felt all

his devices are "connected" since they have to work in "ecosystems" of which he does not have complete control. P7 felt that her computer "has a lot less information on me" than her smartphone but recognized that her smartphone is "synced" to her computer so certain information is shared between the devices – especially for "Google products".

P2 mentioned that she feels that her data is "connected somewhere in the cloud" and that because she uses the same account to set up her Google Home, Smart TV, and smartphone, there is "communication between all the devices". It appears that participants feel that their data is not always kept confidential on a single device.

Also, participants thought not only about how devices share data but also about whether they might be unnecessarily allowing multiple devices to collect the same data. One participant explained that she no longer used dedicated activity trackers because she already had her smartphone with her at all times.

> I was gifted a Fitbit a couple of months ago, and at first I was like, oh, this is super cool. But then it's like, you've got to keep your Bluetooth on and all these things. And I'm like, This is so annoying. And so I used it for like two, three months and now I don't really use it anymore just because it's kind of like I already have my phone at my hip, which is so bad. So I don't want to have like a Bluetooth device and like, you don't need to keep the Bluetooth on. (P7)

When determining comfort with disclosing information or sharing data, participants are thinking not just about which device would collect such information but which devices it might share information with and which devices may already possess such information.

4.3.4 Companies and Brands

Corporations seemed to play a significant role in how comfortable participants were sharing information with their devices (see Figure 4.12). P11 wondered if her "spoken" or "verbal communication" was being "recorded" by her "[cellular service] provider". Participants also referred to their employers as actors who might invade their privacy.

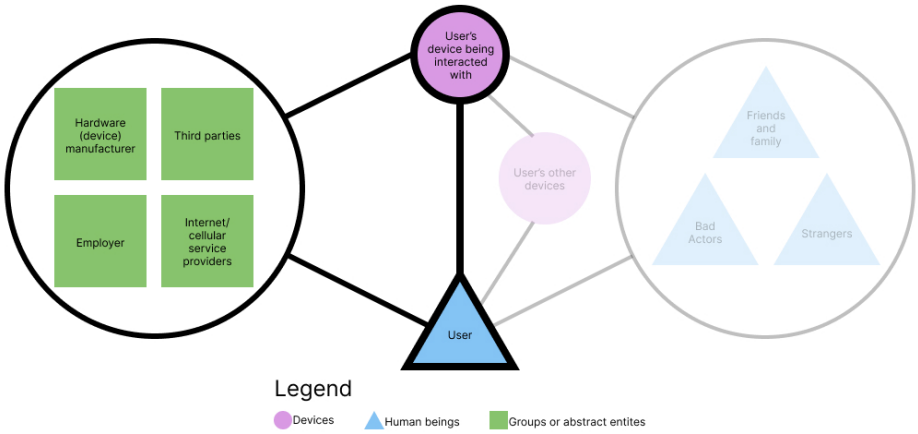

Figure 4.12: Diagram highlighting how participants consider companies or brands in their privacy attitudes and behaviours towards their devices.

P4 said that she and her husband use her computer for personal tasks – instead of her husband's – since she works with her family and not "some corporation who could have access [to her computer]." The perception of a company or brand seemed to influence whether people adopted certain devices. When describing the devices that she used, P7 stated that she is "Team Samsung, so I don't have an iPhone".

In other cases brand perception prevented participants from adopting devices. P7 said that she used to use Dell computers but has stopped after a "creepy and unnerving" experience where a customer service representative from Dell that she was "speaking to looked at [her] address on Google Maps and started commenting on [her] house".

P6 at first expressed interest in having a "dedicated computer" to deal with sensitive information but then said that it would not be fully private since "it's still owned by Microsoft." P6 also expressed some concern about the rise of AI and cloud data sharing on their computer but said they are not too worried because of "trust for Microsoft to do the right thing". Similarly, P4 explained that she was comfortable with having her smartphone know her credit card because she is "very loyal" to Apple and that Apple has "been in [her] life for a long time."

Perception of brand figureheads also affected participants' behaviours. P3 explained that they trust Apple devices to respect their privacy because of Tim Cook:

> [My] level of intelligence versus Tim Cook's level of intelligence, I think

> there's a that's an extreme disparity. So I think that I trust Tim Cook enough to be able to build products that are safe, secure. (P3)

On the other hand, P12 expressed that she "really dislike[s] Amazon" because she "personally hate[s] Jeff Bezos with like a passion" even though she believes that their products are "secure as far as like finances are concerned." Overall, participants' comfort sharing information with their devices was often shaped by their perceptions of companies associated with the devices.

4.4 Limitations

Grounded theory, like all interviewing methodologies, relies on self-reported information from participants. With self-reported data there is always a chance that participants' testimony is inaccurate. Additionally, the pre-screener survey was put up on Prolific and participants who were interested chose to participate, so there may have been some self-selection bias in the recruiting. Additionally, we ran both the interview pre-screener and the previous questionnaire study on Prolific. We used Prolific's built-in participant filtering options to prevent participants who completed the questionnaire study from participating in the interview pre-screener. Moreover, Prolific participants are generally more proficient with technology than the general population; therefore, our set of interview participants are not perfectly representative of the general population. There is a chance that participants were primed for our interviews. Since the primary purpose of the study was investigating CASA, we were not as secretive about the privacy component of the study. We do not mention privacy explicitly in the screener survey, but participants may guess that the interview would relate to privacy based on the inclusion of the trust scale questions in the screener B.

4.5 Conclusion

Our theory about how CASA relates to participants' privacy attitudes and behaviours addresses RQ3, *How, if at all, are people's privacy attitudes explained by CASA?*, and is that:

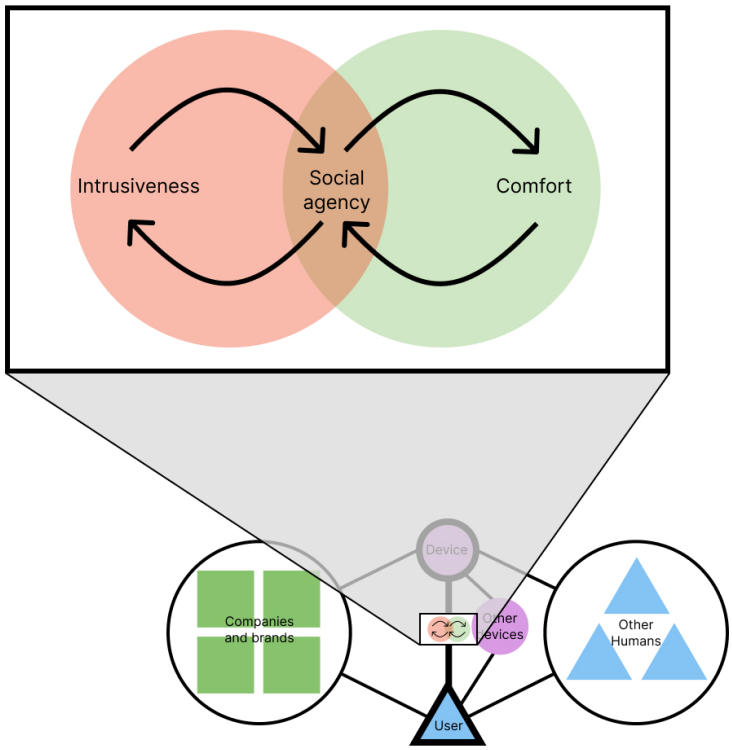

Figure 4.13: Diagram of how figure 4.9 and figure 4.7 relate to each other.

CASA is evident in two types of privacy attitudes: attitudes with constructive or destructive effects. A constructive effect leads participants to trust their device, whereas a destructive effect leads to feelings of distrust and intrusion. Whether an attitude is constructive or destructive largely depends on participants' perceptions of related outside actors.

As indicated in Figure 4.13, the relationships between CASA and privacy attitudes may be cyclical in nature: privacy attitudes reinforcing perceived social agency, and perceived social agency reinforcing privacy attitudes. In our interviews, the outside actors participants referenced were other devices, other humans, and companies.

Participants seemed to feel especially close to their smartphones compared to other devices. They often described their smartphones as extensions of their own bodies or as a close confidant. Participants also explained their comfort sharing sensitive information with their smartphone by referencing the fact that they often have

it nearby and that they are the only person who interacts with their smartphone. For digital assistants, participants were more polarized. Some participants described their digital assistants as they would another person by using human pronouns or attributing differential treatment based on how they spoke to the digital assistant. These participants seemed quite comfortable with the digital assistants being around. Other participants were more concerned about digital assistants and felt that digital assistants intruded into their personal space. Lastly, computers were generally described as an inanimate tool. Participants tended to have fairly neutral feelings about their computer and mostly described computers as a tool for their work.

Chapter 5

Discussion and Conclusion

In this chapter, we summarize the results with respect to our three research questions. Then, we demonstrate the relevance of our findings to recent CASA work. Next, we show the effect of other actors on participants' privacy attitudes and demonstrate a need to adopt a systemic design approach in privacy design. Finally, we outline how this impacts privacy design and we introduce five new CASA-influenced privacy design guidelines.

5.1 Research Questions

Our first study addressed the first 2 research questions. For *RQ1: In which privacy contexts, if any, is social agency attributed to each type of device?*, we found evidence of social agency in four of the seven privacy themes: *Intimacy*, *Solitude*, *Anonymity*, and *Low-self disclosure*. With respect to *RQ2: What differences, if any, exist in people's privacy attitudes towards each type of device?*, we found that attitudes towards digital assistants were significantly different from attitudes towards both computers and smartphones in five of the seven themes; they were also significantly different from the attitudes towards computers in the remaining two themes.

The second study focused on the third research question, *RQ3: How, if at all, are people's privacy attitudes explained by CASA?*. Through the grounded theory interviews we found that CASA influences privacy attitudes in two opposing ways. In some cases, participants seem more comfortable sharing information with devices which they perceive as social actors. we refer to this as a *constructive effect* on privacy attitudes. In other cases, participants are more likely to consider a device intrusive if they perceive it as a social actor. We refer to this as a *destructive effect* on privacy attitudes. In both cases, the relationship between perceived social agency and the privacy attitude seems cyclical. Additionally, it seems that whether the effect is

constructive or *destructive* depends on participants' perception of other related actors such as other devices, other humans, and companies and brands. When determining trust towards another person, one would consider their affiliations and relationships with others [80]. It appears that the same is true here with how participants assess the trustworthiness of devices they perceive to be social actors. However, there are some cases where the device is not perceived as a social actor but the relationship to other actors is still relevant. For example, a device might be a conduit through which a company can spy on the user. In this case the company is the social actor and the device is a conduit for the company to invade the user's privacy.

5.2 Interaction Scripts

In their paper, "Building a Better CASA", Gambino et al. [33] suggest that the previous findings in CASA indicate instances where people follow *human-human interactions scripts* – i.e., common social norms – with devices. They go on to suggest that society may now have had such long term exposure to these devices that specific *human-device scripts* have emerged to guide interaction [33] instead.

In our questionnaire results, we interpret correlations between responses to device questions and person questions as suggesting that the interactions with those devices follow human-human scripts in the given privacy theme. Considering the four themes with correlations, we broadly group them into two contexts. First, *Solitude* and *Intimacy* relate to how much someone allows other social actors into their private social bubble. Secondly, *Low-self disclosure* and *Anonymity* pertain to having other social actors know information about oneself. However, the correlations are generally only moderate: though there seems to be a degree of social agency, we cannot claim with certainty that the interactions exactly follow human-human scripts. It may be that in these privacy contexts, *human-device scripts* have emerged which are substantially similar to CASA's human-human scripts. It also appears that these scripts may vary depending on type of device.

In other privacy contexts, it appears that the human-device scripts may be considerably different than those between humans. In some cases, participants voiced a much stronger desire for privacy from their devices than from other humans, and

these preferences varied significantly depending on the type of device. For example, responses in the *Reserve with Partner* theme suggest that humans have developed a much stronger desire to withhold information from personal devices than from intimate partners. Similarly, responses in *Possessiveness* suggest a much stronger desire to keep personal items and spaces away from personal devices. In both cases, this desire for privacy was strongest for digital assistants.

Our interview results provided greater detail into where new *human-device scripts* occur. Generally, it appeared that participants were applying novel *human-device scripts* to interactions with computers. Participants tended to talk about computers as tools, and, relative to smartphones and digital assistants, were less polarized when discussing their level of comfort sharing personal space and sensitive information with their computers. One common idea which was unique to computers was that participants expressed a greater feeling of control over their computer relative to other devices. This idea of control in relationships is one that may be different in interactions with a device relative to interactions with other humans or social actors.

While modelling novel human-device interaction scripts was not in scope for our thesis, our work highlights some instances where there is need to investigate the interaction scripts that users apply to their interactions with devices. A strong understanding of both the human-human scripts applied to interactions with devices and the novel *human-device scripts* would be valuable in advancing privacy design.

5.3 Building Trusting Relationships

The questionnaire results indicate some key differences in the social agency attributed to the different devices across themes. First, the description for the *Intimacy* theme (see Table 3.1) refers to trusting someone (or in this case, something) with sensitive information. Because trust is such an important component of privacy attitudes, it is interesting to see that only smartphones would follow human-human interactions scripts.

There is a notable discrepancy between the questionnaire and interview results. In the questionnaire, participants attributed social agency to digital assistants in fewer contexts than computers and smartphones. Since digital assistants are voice-based,

one might expect it to elicit treatment most similar to another person. In the interviews, participants seemed to consider digital assistants to be social actors more often than computers but some interview participants expressed significant discomfort towards their digital assistants. We believe that this discrepancy might be the result of the uncanny valley. The uncanny valley [60] is a concept most frequently discussed in robotics and refers to how people are generally comfortable with robots displaying human-like characteristics, until the robots becomes similar enough to appear human yet are is still not quite human, which leads to extreme discomfort. It is important to consider that digital assistants are designed to elicit personification, unlike computers and smartphones. For example, digital assistants encourage verbal conversation in natural language and possess human-like voices. This design aspect of digital assistants may influence the perception of social agency as well as participants' privacy attitudes towards digital assistants. Perhaps digital assistants, with their voice-based interfaces, are similar enough to interactions with real people to fall into an uncanny valley in terms of trust. This discomfort might cause the questionnaire responses for digital assistants to appear distinct from responses about people. Similarly, the uncanny valley may explain why interview participants were uncomfortable with digital assistants and why one described an interaction with a digital assistant as feeling like a "horror film".

There was another case where participants' privacy and trust attitudes towards their device seemed to follow existing social phenomenon. Participants who answered questions about computers and smartphones reported using their device more frequently than those who answered the questions about digital assistants (see Table 3.3). In interviews, participants who tended to share more sensitive information with their smartphones relative to other devices, said that they trusted their smartphone more because they had it with them "at all times". In social psychology, *propinquity* refers to how people are more likely to develop interpersonal relationships when they interact with one another often [28]. This concept has been discussed in social psychology since the 1950s and more recent work [24] has determined that even virtual interactions can influence the likelihood of two people forming a relationship. Therefore, it seems possible that propinquity could play a role in how people interact with and

perceive their devices.

5.4 A Systemic Approach to Privacy Design

Our findings about the role of outside actors on a users' privacy attitudes and behaviours highlight the need for a holistic approach to privacy research and design. Currently, the most prominent set of privacy design principles is Privacy by Design [18]. These principles provide directives for designing digital systems which preserve and respect user privacy. It is important to have clear design guidelines for interactions between a user and a device in privacy interactions; however, the design of this interaction should be complemented by a systemic design approach which incorporates the influence of outside actors.

Systemic design is an approach which seeks to merge systems theory and design and recognizes that both fields have something to contribute to each other [72]. Bornes [13], in a 2023 extended abstract, demonstrates how systemic design can help in addressing complex HCI problems; in her case, sustainable HCI. Notably, cybersecurity literature has already began to incorporate systems theory and socio-technical approaches in discussions of the design and analysis of digital security [91, 92]. Like privacy design, sustainable HCI and cybersecurity are both complex fields which involve many stakeholders with competing interests. Unfortunately, privacy design seems to be lagging behind in its adoption on systemic design or any other system theory concepts relative to those other fields.

We believe that there is an opportunity for privacy design to explore an approach similar to systemic design but which highlights the connection between privacy and social interaction: *Actor-Network Theory (ANT)*. In "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity" [47], Law characterizes ANT as a theory that insists "agents, texts, devices, and architectures" – essentially all peoples and the things they create – "are all generated in, form part of, and are essential to, the networks of the social." In other words, everything, both human and non-human, are actors; all social organizations are made up of a 'network' of actors; and all actors, even non-human, are equal members in social interactions and social system. ANT advocates for this networked view of actors, and calls for researchers to

investigate the ways in which interactions between the actors shape the larger social systems [47].

While ANT was originally developed within and for sociology, it has appeared in several areas of HCI and design research. ANT has been deployed as a lens for advancing participatory design practices [78, 79]. Frauenberger draws on ANT when addressing the types of interactions between humans and computers such as artificial intelligence, virtual reality, and neuro-implants [30]. Storms has connected ANT to the study of algorithms in HCI [77], highlighting the ability for ANT to aid in the study of complex technological systems. This is not an exhaustive look at the connections between ANT and HCI, but we believe that these examples show the value of applying ANT to HCI to better study and design for complex issues. Storms states that ANT "advocates for a radical widening of scope, to include a variety of elements that might otherwise be overlooked but are crucial for a thorough understanding of what is happening." We believe that a "widening of scope" is essential to ensuring that privacy design recognizes the vast set of actors which shape users' privacy attitudes and behaviours.

In the following section, we incorporate ANT in our development of CASA-informed privacy design guidelines. We believe that ANT is an effective tool for privacy research and design because it models privacy as social interactions between a non-hierarchical network of actors. ANT encourages a way of thinking about digital privacy which shines a light the influence of CASA and of outside actors. As such, researchers and designers could more accurately understand users' mental models and behaviours. For example, participants sometimes felt that their digital assistants invaded their privacy. This belief seems ridiculous when starting from the assumption that people have more agency or power than devices; however, an ANT approach, which sees that devices are just as important in a system as other people, recognizes the participant's feelings as completely reasonable. Taking an ANT approach, a design addressing this perspective would prioritize a user's independence from their device. Moreover, the fact that participants take into consideration several actors highlights that privacy involves a *network* of actors and that designs should not be restricted to a single user and single device. If privacy researchers and designers focus

only on the interaction between a user and their device, we will fail to give users the tools they need to fully control their digital privacy.

5.5 Design Implications

Our findings could provide a foundation for future work which uses CASA design principles, possibly adapted to take into account the evolution of human-device scripts, to enhance the usability of privacy and security tools. In "The Man Who Lied to his Laptop", Nass describes how he was able to improve the usability of several digital tools by employing design strategies he learned from his previous work on CASA [63]. CASA has since been applied to address design issues which are close to privacy contexts but never explicitly privacy-related. Kim and Song found that CASA principles can be effectively applied to repair trust in intelligent agents [41]. As mentioned previously, trust is an important consideration for privacy design. Another instance is Alberts and Van Kleek [6]'s 2023 study where they used the CASA paradigm to understand deceptive design patterns. They identify a "social-class" of deceptive design pattern and suggest guidelines for how devices should properly "talk" to users [6]. Deceptive design can negatively impact users' privacy as it can cause users to share information they otherwise would not. The influence of CASA to improve *privacy-adjacent* design suggests the possibility of applying CASA to *privacy-related* design.

We see an opportunity to apply CASA design principles explicitly in privacy-related design; particularly in contexts relevant to *Solitude* or *Low-self disclosure*, because the questionnaire results indicate that users attribute social agency to computers, smartphones, and digital assistants in both these contexts. We propose five high-level privacy design guidelines which are informed by our findings of how CASA affects privacy attitudes.

5.6 CASA-Influenced Privacy Design Guidelines

Leverage privacy design opportunities – and avoid privacy pitfalls – that arise from users' closeness with their device. Like in relationships between human actors, there appears to be different levels of trust in relationships between

humans and devices. The existence of propinquity for relationships with devices could present both risks and opportunities for privacy design. Habituation, the idea that users have decreased responses to repeated stimuli, is a concept often referenced in research about security warnings [39, 82]. If we consider habituation to security warnings when they appear frequently through the lens of propinquity, we might observe that users are less concerned about warnings they see often. Propinquity could also be used as a lens for understanding some cases of social engineering. Users may tend to trust and disclose information more readily on familiar devices, which could be leveraged by malicious attackers. Conversely, this could plausibly be incorporated into privacy design by fostering a relationship and encouraging users to only share information in specific contexts or in the presence of devices with enhanced security or privacy protocols.

Ensure that users can interact with their smartphones privately. We found that users will be most comfortable sharing sensitive information with their smartphone relative to their computer or digital assistant. In the *Intimacy* theme, only responses to questions about smartphones correlated with the matched questions about humans. Therefore, participants seem to expect that their interactions with their smartphones are confidential. This was echoed in the interviews. Many interview participants felt comfortable sharing sensitive information such and their credit cards with their smartphone. Moreover, some participants expressed that they and their partner keep their device private even from each other. Therefore, when a user shares information with their smartphone, it should not be shared with other actors, neither devices nor humans, by default. Consequently, they might use their smartphones for more personal or confidential activities such as online banking or managing personal photos. On the negative side, users could be particularly vulnerable to phishing attempts or privacy-compromising deceptive design patterns when using their smartphone.

Design devices to respect users' personal space. The questionnaire results suggest that all devices can intrude upon users when they want to be alone (physically or mentally). In the interviews, some participants described disabling their digital

assistant when they wanted to have privacy. Others mentioned that they hide their work devices when they finish working for the day. It is important to ensure that users are able to disconnect – and confirm that they have in-fact disconnected – from their devices, particularly digital assistants since questionnaire responses indicated greater desire for *Solitude* from digital assistants relative to the other devices. It might benefit users to provide easy, transparent mechanisms for managing sensors, such as cameras or microphones, on their device to foster the feeling that users can disconnect from their device. This principle could complement proposals such as Ahmad et al.'s [5] call for tangible on-off switches to control the sensors built into digital assistants. Features such as the sensor indicators on iOS [7] or the "on" light next to the camera on MacBooks [8] can also help users verify that their devices are not intruding. However, the absence of a cue may be insufficient to reassure users — an additional explicit "off" indicator or cover would be preferable. We see evidence of this need from the number of participants who described covering their computer's webcam with third-party camera covers or tape when not in use. Other sensors which do not rely of visual input, such as microphones, are even more difficult for users to disable or hide from. It is critical that such features are not vulnerable to mis-activation as it may lure users into false feelings of solitude.

Respect the device's perceived individuality – or lack-thereof. The social agency of computers and smartphones in the *Anonymity* theme indicates that users consider each of these devices as different agents. In the interviews, participants mentioned using dedicated computers and smartphones for their work which they did not do personal tasks on. Similarly, some participants mentioned their family members having their own dedicated computers and smartphones. In other words, work devices and personal devices are considered to be different actors. However, participants tended to describe their digital assistants as a single entity, even when they owned multiple speakers for interacting with the digital assistant. This aligns with the findings of Nass et al. [62], which show that people treat different voices as different social actors and recognize a repeated voice as a single entity. Therefore, it may be desirable to ensure that users are given control over which specific smartphones or computers have access to information. On the other hand, users may perceive

multiple digital assistants as being the same agent since digital assistants are designed to exist seamlessly across multiple physical devices (e.g., consider a home with digital assistants in several rooms). When designing for digital assistants, designers should treat all the physical devices as part of the same single entity. For example, users may prefer to manage privacy settings for digital assistants with a single set of parameters rather than unique parameters per physical device.

Match disclosure requests to appropriate devices. Users may be comfortable sharing sensitive information with one device but not with other devices. Given the correlations in the *Low-self disclosure* theme – and the relatively high desire for privacy – we propose that sharing information with a device follows similar social scripts as sharing information with another person. Given that the digital assistant responses were significantly lower than the computer responses for the *Low-self disclosure* theme, designers should be aware that they might face resistance in getting users to share sensitive information with their digital assistants relative to their computer. Moreover, many interview participants used their smartphone for sensitive tasks like online banking but were uncomfortable using other devices for this task. Therefore, tasks requiring sensitive information, such as financial or health services which involve sensitive data, should be available for completion on smartphones. Since participants consider a network of actors in their privacy interactions, it might even be preferable to move a task from some other device onto a smartphone when the task requires sensitive information.

5.7 Future Work

Firstly, we would like do future work to validate our theory of CASA's influence on privacy attitudes and behaviours. Observing the original CASA studies more closely, we envision running a controlled study where participants interact with devices which are designed to elicit different levels of social agency and which would be associated with different outside actors (e.g. different brands). Similarly, it would be worth validating our proposed design principles. A future study could generate two designs: one adhering to the CASA-based privacy design principles and one breaking them,

and have users evaluate the two designs.

The fact that people interacted with their phones frequently appeared as a justification for why they shared sensitive information with their phone. It would be valuable to run another study which relative attitudes of participants who interact with their devices at different frequencies.

During interviews, participants referred to some devices beyond the three we set out to study: such as smartwatches or IoT enabled appliances. Future work should investigate the relationship between CASA and privacy for devices other than computers, smartphone, or digital assistants. In a similar vein, some participants referenced interacting with their digital assistant through secondary devices such as their smartphone or smart watch. It could be valuable to study how changes in the physical device affect perceived social agency.

Finally, we mentioned that capturing detailed models of human-device interaction scripts was out of scope for our thesis. In the future, it would be useful to build a deeper understanding of the new interaction scripts that users apply to interactions with devices. Having a clear model of when users apply human-device scripts and when they apply human-human scripts in privacy interactions could help designers apply CASA design concepts to privacy more precisely and effectively.

5.8 Conclusion

In conclusion, CASA does influence some privacy attitudes and behaviours. Through an online questionnaire, we found four privacy themes, *Intimacy*, *Solitude*, *Anonymity*, and *Low-self disclosure*, in which participants treated their computers, smartphones, or digital assistants as social actors. Through grounded theory interviews, we developed a theory that explains how some of participants' privacy attitudes related to CASA. Our theory is that:

> *CASA is evident in two types of privacy attitudes: attitudes with constructive or destructive effects. A constructive effect leads participants to trust their device, whereas a destructive effect leads to feelings of distrust and intrusion. Whether an attitude is constructive or destructive largely depends on participants' perceptions of related outside actors.*

While we found some evidence of CASA in privacy interactions, the results suggest other factors also influence privacy attitudes. Given the ubiquitous nature of technology today, it is possible that CASA now manifests differently. Based on these findings, we suggest incorporating Actor-Network theory into digital privacy research and design. Finally, we developed a set of CASA-informed privacy design principles. CASA as a theory has had a significant influence on the field of HCI; we have shown that CASA should receive more attention in privacy research and design. While the current privacy design approach has been useful in promoting user privacy, our findings indicate that researchers and designers must adopt a more systemic design approach to properly match users' privacy attitudes and behaviours.

Bibliography

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *Symposium On Usable Privacy and Security (SOUPS)*, 2019.

[2] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L Mazurek. Comparing security and privacy attitudes among us users of different smartphone and smart-speaker platforms. In *Symposium On Usable Privacy and Security (SOUPS)*, 2021.

[3] Alessandro Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*, pages 21–29, 2004.

[4] Alan Agresti. *Analysis of ordinal categorical data*. John Wiley & Sons, 2010.

[5] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):116:1–116:28, October 2020.

[6] Lize Alberts and Max Van Kleek. Computers as bad social actors: Dark patterns and anti-patterns in interfaces that act socially. *arXiv preprint arXiv:2302.04720*, 2023.

[7] Apple. Control access to hardware features on iPhone.

[8] Apple. Don't close your MacBook, MacBook Air, or MacBook Pro with a cover over the camera, October 2022.

[9] Fenye Bao and Ing-Ray Chen. Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things*, Self-IoT '12, pages 1–6, New York, NY, USA, September 2012. Association for Computing Machinery.

[10] Fenye Bao and Ray Chen. Trust management for the internet of things and its application to service composition. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–6. IEEE, 2012.

[11] Susanne Barth and Menno DT De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and informatics*, 34(7):1038–1058, 2017.

[12] Zinaida Benenson and Lena Reinfelder. Should the users be informed? on differences in risk perception between android and iphone users. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 1–2, 2013.

[13] Laetitia Bornes. A methodology and a tool to support the sustainable design of interactive systems: Adapting systemic design tools to model complexity in interaction design. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–5, 2023.

[14] danah boyd and Alice E Marwick. Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A decade in internet time: Symposium on the dynamics of the internet and society*, 2011.

[15] Astrid Carolus, Jens F Binder, Ricardo Muench, Catharina Schmidt, Florian Schneider, and Sarah L Buglass. Smartphones as digital companions: Characterizing the relationship between users and their phones. *New Media & Society*, 21(4):914–938, April 2019. Publisher: SAGE Publications.

[16] Astrid Carolus, Ricardo Muench, Catharina Schmidt, and Florian Schneider. Impertinent mobiles - Effects of politeness and impoliteness in human-smartphone interaction. *Computers in Human Behavior*, 93:290–300, April 2019.

[17] Astrid Carolus, Catharina Schmidt, Florian Schneider, Jule Mayr, and Ricardo Muench. Are People Polite to Smartphones? In Masaaki Kurosu, editor, *Human-Computer Interaction. Interaction in Context*, volume 10902, pages 500–511. Springer, Cham, 2018.

[18] Ann Cavoukian. Privacy by design: The 7 foundational principles, 2009.

[19] George Chalhoub and Ivan Flechais. "alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In *HCI for Cybersecurity, Privacy and Trust*, pages 305–325. Springer, Cham, 2020.

[20] Kathy Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis*. Sage, 2014.

[21] Sonia Chiasson and Carl Gutwin. Testing the media equation with children. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, pages 829–838, New York, NY, USA, April 2005. Association for Computing Machinery.

[22] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 331–346, 2022.

[23] Alan E. Craddock. The measurement of privacy preferences within marital relationships: The relationship privacy preference scale. *The American Journal of Family Therapy*, 25(1):48–54, March 1997.

[24] Ted Michael Dickinson. *An Inefficient Choice: An Empirical Test of Media Richness and Electronic Propinquity*. PhD thesis, The Ohio State University, 2012.

[25] Tobias Dienlin, Philipp K Masur, and Sabine Trepte. A longitudinal analysis of the privacy paradox. *New Media & Society*, page 14614448211016316, 2021.

[26] Robert A Fahey and Airo Hino. Covid-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, 55:1–5, 2020.

[27] Adrienne Porter Felt, Serge Egelman, and David Wagner. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, pages 33–44, 2012.

[28] Leon Festinger, Stanley Schachter, and Kurt Back. *Social pressures in informal groups; a study of human factors in housing*. Social pressures in informal groups; a study of human factors in housing. Harper, Oxford, England, 1950.

[29] Jonas Foehr and Claas Christian Germelmann. Alexa, Can I Trust You? Exploring Consumer Paths to Trust in Smart Voice-Interaction Technologies. *Journal of the Association for Consumer Research*, 5(2):181–205, April 2020. Publisher: The University of Chicago Press.

[30] Christopher Frauenberger. Entanglement hci the next wave? *ACM Transactions on Computer-Human Interaction (TOCHI)*, 27(1):1–27, 2019.

[31] Nathaniel Fruchter and Ilaria Liccardi. Consumer attitudes towards privacy and security in home assistants. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

[32] Diego Gambetta et al. Can we trust trust. *Trust: Making and breaking cooperative relations*, 13(2000):213–237, 2000.

[33] Andrew Gambino, Jesse Fox, and Rabindra Ratan. Building a Stronger CASA: Extending the Computers Are Social Actors Paradigm. *Human-Machine Communication*, 1:71–86, February 2020.

[34] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, 77:226–261, 2018.

[35] Julie M Haney, Susanne M Furman, and Yasemin Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22*, pages 393–411. Springer, 2020.

[36] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 2016.

[37] Chris Jay Hoofnagle, Jennifer M Urban, and Su Li. Mobile payments: Consumer benefits & new privacy concerns. *Available at SSRN 2045580*, 2012.

[38] Sharon Jackson. Toward an analytical and methodological understanding of actor-network theory. *Journal of Arts and Humanities*, 4(2):29–44, 2015.

[39] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention. *ACM Transactions on Privacy and Security*, 23(1):5:1–5:38, February 2020.

[40] Amy K Karlson, AJ Bernheim Brush, and Stuart Schechter. Can i borrow your phone? understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1647–1650, 2009.

[41] Taenyun Kim and Hayeon Song. How should intelligent agents apologize to restore trust? Interaction effects between anthropomorphism and apology attribution on trust repair. *Telematics and Informatics*, 61:101595, August 2021.

[42] Jennifer King. How come i'm allowing strangers to go through my phone? smartphones and privacy expectations. *Smartphones and Privacy Expectations.(March 15, 2012)*, 2012.

[43] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A Martucci. Enhancing privacy through the visual design of privacy notices: exploring the interplay of curiosity, control and affect. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, pages 437–456, 2020.

[44] Rex B. Kline. *Principles and practice of structural equation modeling*. Methodology in the social sciences. The Guilford Press, New York, fourth edition edition, 2016.

[45] Jacob Leon Kröger and Philip Raschke. Is my phone listening in? on the feasibility and detectability of mobile eavesdropping. In *Data and Applications Security and Privacy XXXIII*, pages 102–120. Springer, Cham, 2019.

[46] Stan Kurkovsky and Ewa Syta. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In *2010 IEEE International Symposium on Technology and Society*, pages 441–449. IEEE, 2010.

[47] John Law. Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems practice*, 5:379–393, 1992.

[48] Scott Lederer, Jennifer Mankoff, and Anind K Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*, pages 724–725, 2003.

[49] Jong-Eun Roselyn Lee and Clifford I. Nass. Trust in computers: The computers-are-social-actors (CASA) paradigm and trustworthiness perception in human-computer communication. In *Trust and technology in a ubiquitous modern environment: Theoretical and methodological perspectives*, pages 1–15. IGI Global, 2010.

[50] Seth C. Lewis, Andrea L. Guzman, and Thomas R. Schmidt. Automation, Journalism, and Human–Machine Communication: Rethinking Roles and Relationships of Humans and Machines in News. *Digital Journalism*, 7(4):409–427, April 2019. Publisher: Routledge _eprint: https://doi.org/10.1080/21670811.2019.1577147.

[51] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. Understanding the role of privacy and trust in intelligent personal assistant adoption. In *Information in Contemporary Society: 14th International Conference, iConference 2019, Washington, DC, USA, March 31–April 3, 2019, Proceedings 14*, pages 102–113. Springer, 2019.

[52] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In *Information in Contemporary Society*, Lecture Notes in Computer Science, pages 102–113, Cham, 2019. Springer International Publishing.

[53] Matthew Lombard and Kun Xu. Social Responses to Media Technologies in the 21st Century: The Media are Social Actors Paradigm. *Human-Machine Communication*, 2(1), April 2021.

[54] Christoph Lutz and Gemma Newlands. Privacy and smart speakers: A multidimensional approach. *The Information Society*, 37(3):147–162, 2021.

[55] Maria Madsen and Shirley Gregor. Measuring Human-Computer Trust. In *11th australasian conference on information systems*, volume 53, pages 6–8, 2000.

[56] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4):336–355, December 2004. Publisher: INFORMS.

[57] Nancy J. Marshall. DIMENSIONS OF PRIVACY PREFERENCES. *Multivariate Behavioral Research*, 9(3):255–271, July 1974.

[58] Graeme McLean and Kofi Osei-Frimpong. Hey Alexa ... examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior*, 99:28–37, October 2019.

[59] Josipa Milas and Gordana Lesinger. The relationship between the perception of advertising, fomo, social network fatigue and privacy concerns among social network users. *Communication Management Review*, 7(01):26–47, 2022.

[60] Masahiro Mori, Karl F. MacDorman, and Norri Kageki. The Uncanny Valley [From the Field]. *IEEE Robotics & Automation Magazine*, 19(2):98–100, June 2012.

[61] Clifford Nass and Youngme Moon. Machines and mindlessness: Social responses to computers. *Journal of social issues*, 56(1):81–103, 2000.

[62] Clifford Nass, Jonathan Steuer, and Ellen R. Tauber. Computers are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '94, pages 72–78, New York, NY, USA, April 1994. Association for Computing Machinery.

[63] Clifford Nass and Corina Yen. *The Man Who Lied to His Laptop: What We Can Learn About Ourselves from Our Machines*. Penguin, September 2010.

[64] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126, 2007.

[65] Jonghwa Park, Hanbyul Choi, and Yoonhyuk Jung. Users' cognitive and affective response to the risk to privacy from a smart speaker. *International Journal of Human–Computer Interaction*, 37(8):759–771, 2021.

[66] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. A deep dive into user's preferences and behavior around mobile phone sharing. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–22, 2023.

[67] Darhl M. Pedersen. Dimensions of Privacy. *Perceptual and Motor Skills*, 48(3_suppl):1291–1297, August 1979.

[68] Valentina Pitardi and Hannah R. Marriott. Alexa, she's not human but... Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology & Marketing*, 38(4):626–642, 2021.

[69] Andrew K Przybylski, Kou Murayama, Cody R DeHaan, and Valerie Gladwell. Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in human behavior*, 29(4):1841–1848, 2013.

[70] Byron Reeves and Clifford Ivar Nass. *The media equation: how people treat computers, television, and new media like real people and places*. CSLI Publications ; Cambridge University Press, Stanford, Calif. : New York, 1996.

[71] Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina. Internet. *Our World in Data*, July 2015.

[72] Birger Sevaldson. What is systemic design? practices beyond analyses and modelling. In *Relating Systems Thinking and Design (RSD8) 2019 Symposium*, 2019.

[73] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 807–816, 2015.

[74] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76:146–164, January 2015.

[75] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167–196, 1996. Publisher: Management Information Systems Research Center, University of Minnesota.

[76] Daniel J Solove. The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89:1, 2021.

[77] Elias Storms. Exploring actor-network theory in the investigation of algorithms. In *ACM CHI Conference on Human Factors in Computing Systems*, 2019.

[78] Cristiano Storni, Thomas Binder, Per Linde, and Dagny Stuedahl. Designing things together: intersections of co-design and actor–network theory, 2015.

[79] Cristiano Storni, Per Linde, Thomas Binder, and Dagny Stuedahl. Exploring ant in pd: reflections and implications for theory and practice. In *Proceedings of the 12th Participatory Design Conference: Exploratory Papers, Workshop Descriptions, Industry Cases-Volume 2*, pages 145–146, 2012.

[80] Isabel Thielmann and Benjamin E Hilbig. Trust: An integrative review from a person–situation perspective. *Review of General Psychology*, 19(3):249–277, 2015.

[81] Ruben Geert van den Berg. Kendall's Tau - Simple Introduction.

[82] Anthony Vance, Jeffrey L. Jenkins, Bonnie Brinton Anderson, Daniel K. Bjornn, and C. Brock Kirwan. Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments. *MIS Quarterly*, 42(2):355–380, February 2018.

[83] Ari Ezra Waldman. *Privacy as trust: Information privacy for an information age*. Cambridge University Press, 2018.

[84] Alan F Westin. Privacy and freedom. *Washington and Lee Law Review*, 25(1):166–170, 1968.

[85] Alan F Westin. Social and political dimensions of privacy. *Journal of social issues*, 59(2):431–453, 2003.

[86] Fiona Westin and Sonia Chiasson. "it's so difficult to sever that connection": The role of fomo in users' reluctant privacy behaviours. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2021.

[87] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12):1, 2011.

[88] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John Millar Carroll. Measuring mobile users' concerns for information privacy. In *International Conference on Interaction Sciences*, 2012.

[89] Toshio Yamagishi, Masako Kikuchi, and Motoko Kosugi. Trust, Gullibility, and Social Intelligence. *Asian Journal of Social Psychology*, 2(1):145–161, 1999.

[90] Toshio Yamagishi and Midori Yamagishi. Trust and commitment in the united states and japan. *Motivation and emotion*, 18(2):129–166, 1994.

[91] Dingyu Yan. A systems thinking for cybersecurity modeling, 2020.

[92] Erjon Zoto, Mazaher Kianpour, Stewart James Kowalski, and Edgar Alonso Lopez-Rojas. A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, 50(18):65–75, 2019.

Appendix A

Study 1: Survey Questions

Demographics

1. Which of the following best describes your gender identity? *Man, Non-binary, Woman, Not listed above [please specify], Prefer not to say*
2. Age in years _____
3. How would you describe your computer skills?
   Basic skills: *I can turn on and off a computer; edit, save and print files; navigate websites; send an email;*
   Intermediate skills: *I can recognize and save files in various format (such as .pdf, .doc, .jpg, .html, etc.); add (and save) attachments to email; complete online forms; download files from the Internet; create bookmarks to organize browsed pages; customize software tools;*
   Advanced skills: *I can attach and use peripheral devices (scanners, printers, media storage); check file properties to determine memory size, install some software; use the history feature in web browsers; use function keys and keyboard shortcuts; recognize spam;*
   Proficient skills: *I have formal computer science background and/or significant working experience in this area;*
   Prefer not to answer
4. Which of the following devices do you own:
   Computer *a desktop or laptop with which you are able to connect to the internet or complete basic computational task such as word processing (e.g. Desktop PC, Macbook, Dell Laptop, etc);*
   Smartphone *a portable computing device which is able to accomplish telecommunication tasks such as calling and texting as well as connect to the internet (e.g iPhone, Blackberry, Samsung Galaxy, etc);*
   Digital Assistant *A digital assistant which operates from its own dedicated hardware and NOT from a phone or computer (e.g. Amazon Alexa, Google Home, Apple Home Pod, etc).*
5. How often do you use your (computer/smartphone/digital assistant)? *Everyday, 4-6 days a week, 2-3 days a week, Once a week, Other: please explain*

Questions

Please indicate your level of agreement with the following statements

*All questions are 5-point Likert scale questions (strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree). * indicates that a question is reverse coded. Cells highlighted in red were excluded from final analysis as part of the factor analysis process.*

ID	Person Question	Device Question
IN-i	People should respect other's right to be individual and different.	Devices should respect people's right to be individual and different.
IN-1	It is important to be able to confide in someone and know that your confidence will be kept secret.	It is important to be able to confide in a device and know that your confidence will be kept secret.

IN-2	Even intimate friends should respect your desire to keep certain things to yourself.	Even personal devices should respect your desire to keep certain things to yourself.
IN-3	Close friendships require having time to be alone together.	A personal device is one that you spend time alone with.
IN-4	I occasionally enjoy getting away from the rest of the world with an intimate friend.	I occasionally enjoy getting away from the rest of the world with a personal device.
IN-5	It is very relaxing to get away from other people with just your family or close friends.	It is very relaxing to get away from other people with just my personal device.
IN-6	I like to have someone to whom I can tell everything about myself, even my deepest thoughts and feelings.	I like to have a device to whom I can share everything about myself, even my deepest thoughts and feelings
IN-7	Even members of a family need to get away from each other every now and then.	I need to get away from my devices every now and then.
IN-ii*	I have a special person that I can confide in.	I have a personal device that I share personal information with.
IN-iii*	I like my friends to sympathize with me and to cheer me up when I am depressed.	I would like my devices to sympathize with me and to cheer me up when I am depressed.
IN-iv*	It pleases me when my accomplishments obtain recognition from others.	It pleases me when my devices recognize my accomplishments
NN-1*	I want my friends to feel that they can drop in at my house any time they like.	I want my devices to be able to get my attention whenever they like.
NN-2*	I really enjoy being able to loan things to friends.	I really enjoy being able to share information with my devices.
NN-i	Although I occasionally enjoy talking to my neighbours, I don't like to get very involved with them.	Although I occasionally enjoy interacting with my devices, I don't like to get very involved with them.
NN-3*	When I really need to find a solution for a problem, I do it best by talking with others rather than working alone.	When I really need to find a solution for a problem, I do it best by interacting with my devices rather than working alone.
SE-i	I would like to live in a secluded house out of sight of any other houses.	I would like to live in a secluded house away from of any devices.
SE-ii	I would like to have a private retreat which no one would enter without asking me.	I would like to have a private retreat which no devices would activate without my permission.
SE-iii	I like to go on vacation alone with my family.	I like to go on vacation alone with my devices.
SE-iv	I prefer doing things with only my family.	I prefer doing things with only my devices.
SE-v	I do not like to be disturbed when I am at home engaged in a family activity.	I do not like to be disturbed when I am at home engaging with my devices.
SE-vi	I would like to have a mountain cabin where my family and I could be alone together.	I would like to have a mountain cabin where I could be alone with my devices.
SO-1	I sometimes want to get away from everyone for a while, even my close friends.	I sometimes want to get away from everyone for a while, even my personal device.

SO-2	There are times when I really want other people to leave me alone and not intrude on my thought even though we're in the same room.	There are times when I really want my device to leave me alone and not intrude on my thoughts even though we're in the same room.
SO-3	I need a lot of time to be alone, even from my partner.	I need a lot of time to be alone, even from my personal device.
SO-i*	I don't need a lot of opportunities to be apart from other people.	I don't need a lot of opportunities to be apart from my personal device.
SO-4	I prefer to have a lot of time to get away from other people and just be on my own.	I prefer to have a lot of time to get away from my device and just be on my own.
SO-ii	I would like to work in a fire watch tower all by myself for a summer.	I would like to work in a fire watch tower away from my devices for a summer.
SO-5	I sometimes need to be alone and away from anyone.	I sometimes need to be alone and away from my devices.
SO-6	I like to be home with nobody else around.	I like to be home and have none of my devices bothering me.
SO-7	Sometimes I like to be alone where I cannot be observed by anyone.	Sometimes I like to be alone where I am detached from my devices.
AN-1	I would like to have acquaintances at work, at home, in clubs, and so forth that don't know each other because each group would only know a part of me.	I would like to have devices at work, at home, in clubs, and so forth that don't communicate with each other because each group would only know a part of me.
AN-2	I often like to go to a secluded place to talk to an intimate friend.	I often like to go to a secluded place to communicate with a personal device.
AN-i*	I like other people to notice me when I am in public.	I like when devices are aware of me in public.
LD-1	I dislike talking about personal matters to a friend in a crowded place where other people can overhear us.	I dislike sharing personal information with my device in a crowded place where other people can overhear us.
LD-2	I usually don't tell people I don't know very well personal things about myself.	I usually don't share personal information with devices I have not often engaged with.
LD-3	I don't like to talk about personal things with friends until I have known them a long time.	I don't like to share personal information with devices until I am familiar with them.
LD-4	I would be very upset if someone read something I had written or my personal correspondence without my permission.	I would be very upset if my device read something I had written or my personal correspondence without my permission.
LD-i	Acquaintances often ask questions that I consider rude and personal.	Devices often ask questions that I consider intrusive and personal.
LD-5	I would be reluctant to engage in a prolonged conversation with someone I had just met.	I would be reluctant to have a prolonged interaction with a device I had not engaged with before.
RP-1*	I think it is important to tell my partner just about everything there is to know about me.	I think it is important to share all of my information with my personal devices.
RP-2*	It is important for me to confide in my partner about my work life.	It is important for me to share information about my work life with my personal device.

RP-3	My personal preference is not to tell my partner all my deepest feelings.	My personal preference is not to share my deepest feelings with my device.
PO-1*	My partner doesn't have to ask to borrow my things.	My personal devices shouldn't have to ask for access to my information.
PO-2	I feel uncomfortable letting my partner borrow things that are special to me.	I feel uncomfortable letting my devices access information that is special to me.
PO-i*	I like to meet new people.	I like to engage with new devices.

Debrief

Thank you for completing this survey!

The purpose of this study was to investigate the relationship between Computers Are Social Actors (CASA) and privacy. Computers Are Social Actors (CASA) is a phenomenon where humans unconsciously act towards computers as they would towards other humans. Most work with CASA has involved comparisons between how users respond to computers compared to how they respond to human-human interaction. CASA is well understood, however, there is a gap in understanding the relationship between CASA and digital privacy.

This survey was composed of questions from psychology privacy preference questionnaires. Each question had one version which looked at interactions between two people and one version which looked at interactions between a person and a device.

Appendix B

Study 2: Pre-Screener

Demographics

1. Which of the following best describes your gender identity?
   - Man
   - Non-binary
   - Woman
   - Not listed (Please specify)
   - Prefer not to say
   - Age in years? [Textbox]
2. In which province are you currently living? [Textbox]
3. Do you have experience in computer science, information technology, computer/software engineering, or a related field?
   - Yes (please briefly describe) [Textbox]
   - No
4. Which of the following devices do you use? (select all that apply)
   Computer: a desktop or laptop computer that connects to the internet (e.g. Desktop PC, MacBook, Dell Laptop).
   Smartphone: a smartphone which can be used to make phone calls, send text messages, and connect to the internet (e.g iPhone, Blackberry, Samsung Galaxy.
   Digital Assistant: A physical digital assistant which operates from its own dedicated hardware (e.g. Amazon Alexa, Google Home, Apple Home Pod). This does NOT assistants built-in to a phone or computer

Questions 5, 6, and 7 will be displayed based on the response to question 4 to ensure that participants are only asked about devices which they use.

5. How often do you use computers?
   - Everyday
   - 4-6 days a week
   - 2-3 days a week
   - Once a week
   - Other: please explain [Textbox]

6. How often do you use smartphones?
    Everyday
    4-6 days a week
    2-3 days a week
    Once a week
7. How often do you use digital assistants (e.g. Amazon Alexa, Google Home, Apple Home Pod, etc)?
    Everyday
    4-6 days a week
    2-3 days a week
    Once a week
    Other: please explain [Textbox]

Trust Scale

The following questions all follow a 5-point Likert scale (Strongly disagree, Somewhat disagree, Neutral, Somewhat agree, Strongly agree)

1. Most people are basically honest
2. Most people are trustworthy
3. Most people are basically good and kind
4. Most people are trustful of others
5. I am trustful
6. Most people will respond in kind when they are trusted by others

Appendix C

Study 2: Interview Guide

Introduction

Intent: Understand context about the participants and their relationships with their devices.

1. Can you tell me a bit about your experience with technology?

Trust and Relationships with Devices

Intent:

I. *To what degree do participants use social actor language to describe interactions with their devices.*
II. *Understanding whether users have more trust for some devices over others.*

Computer/Phone/Digital Assistant --- repeat for each type of device

1. (*I*) How does your computer fit into your life? Generally, what do you use them for?
2. (*II*) What information about you can your computer access?
    a. How do you feel about it having access to that info?

All devices

1. (*II*) If you needed to access sensitive information (i.e., financial or health information) which device would you be most likely to use?
    a. Why did you choose that device over the others?
2. (*II*) How much do you trust your devices? Can you tell me more about this?
    a. What makes you trust one device more than another?
3. (I) Have you ever felt that you misplaced trust in a device?
    a. Can you tell me more about this?

Privacy Attitudes and Behaviors

Intent:

I. *Understanding how general perceptions of devices as social actors might influence participants' privacy attitudes. (e.g. Do they hold similar privacy attitudes towards their devices and other human-beings?)*
II. *Understanding the blame participants attribute to their devices in privacy breaches and if non-human devices are able to invade their privacy.*

1. (*I*) Are your interactions with each of your devices confidential? Why?
    a. Who or what might be observing the interactions?
    b. What actions do you take to increase your privacy?
2. (*I*) Have you ever felt that your privacy was violated while using your devices?
    a. Can you tell me more about this?
    b. In this case, who would you blame for the privacy violation?
3. (*I*) Are there things you do to protect your privacy or security when using one device but not others? Why?
4. (*I*) Is there any sensitive information you hide from access on one device but not others? Why?
5. (*I*) Are there sensitive tasks you would do with a device rather than with another person? Why?
    a. Are there cases where you would prefer to interact with a person rather than a device? Why?
6. (*I*) If you think about your <device> can you describe how your privacy might be invaded?
7. (*II*) Have you ever experienced a situation where your camera or microphone was activated without your knowledge? Can you tell me more about this?

Conclusion

1. That brings us to the end of the interview, is there anything else you'd like to share about this topic?
2. Do you have any questions for me before we end?