Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption

Yuting Liao[1], Jessica Vitak[1], Priya Kumar[1], Michael Zimmer[2], and Katherine Kritikos[2]

[1]University of Maryland, College Park, MD 20742, USA
{yliao598, jvitak, pkumar12}@umd.edu

[2] University of Wisconsin—Milwaukee, Milwaukee, WI 53211, USA
{zimmerm, kritikos}@uwm.edu

Abstract. Voice-controlled intelligent personal assistants (IPAs) have seen tremendous growth in recent years on smartphones and as standalone devices in people's homes. While research has examined the potential benefits and drawbacks of these devices for IPA users, few studies have empirically evaluated the role of privacy and trust in individual decision to adopt IPAs. In this study, we present findings from a survey of IPA users and non-users (N=1160) to understand (1) the motivations and barriers to adopting IPAs and (2) how concerns about data privacy and trust in company compliance with social contract related to IPA data affect acceptance and use of IPAs. We discuss our findings in light of social contract theory and frameworks of technology acceptance.

Keywords: Intelligent Personal Assistant; Internet of Things; Privacy; Technology Adoption; Amazon Alexa; Google Home; Social Contract Theory

1 Introduction

As a component of the Internet of Things (IoT) ecosystem, voice-controlled intelligent personal assistants (IPAs) have seen tremendous growth in recent years, with nearly half (47%) of Americans saying they now use an IPA on their smartphone or in their home [24]. IPAs—including Apple's Siri, Amazon's Alexa, and Google's Assistant—are increasingly being integrated into many consumer mobile devices, vehicles, and homes, as well as university dorms and hotels [28, 33].

Utilizing artificial intelligence, machine learning, and natural language processing techniques, IPAs facilitate information retrieval by providing information based on user input (e.g., offering weather updates) and acting on behalf of users to complete tasks (e.g., turning on/off lights at home). Despite these potential benefits, IPAs raise several security and privacy challenges for consumers. IPAs rely on cloud computing, with devices transmitting a large amount of users' behavioral data—including real-time voice data—through the internet to remote cloud servers. In the event of a data breach, an adversary could access users' detailed IPA usage history and potentially infer additional information about users' lifestyles and behavioral patterns through data mining techniques [4, 8]. Researchers have also identified privacy concerns among users who control their smart home appliances via IPA devices, including continuous audio/video recording, data collection and mining, adversarial remote control, and network attacks on local devices [35].

In general, previous IPA studies have been conducted in a particular socio-technical context using qualitative methods with a small number of users and ignoring the non-user population. Thus, their findings limit our ability to understand broader attitudes toward IPAs among users and non-users alike, as well as why some people may adopt these technologies while others do not. To begin to address these gaps, we conducted a survey with 1178 users and non-users of IPAs in the United States to investigate factors that affect adoption of IPAs, with a special focus on the role privacy and trust play in decision-making processes. Specifically, we ask the following research questions:

> ***RQ1:*** *What are the motivations and barriers for people to adopt IPA devices?*
>
> ***RQ2:*** *What differences—if any—exist between people who use IPAs and those who do not?*
>
> ***RQ3:*** *How are individual characteristics and privacy attitudes associated with non-users' behavioral intention to adopt a Home IPA?*[1]

In the following sections, we synthesize the existing research on IPAs, as well as present our theoretical frameworks—privacy as social contract and technology acceptance model—for interpreting the data. After describing our findings, we discuss them through the lens of these frameworks. We argue that a deeper and more robust understanding of the privacy and trust implications of IPA adoption and use will provide critical insights into the design of future voice-controlled IPAs—as well as IoT devices in general, which will see significant growth over the next decade.

2 Related Work

2.1 Research on IPAs, Privacy, and Trust

Research in information science and human-computer interaction has explored various social dimensions of the current generation of IPAs, including how people use these devices at home [3] and in group conversation [25], whether users personify their devices [14, 27], how children interact with the devices [9], and how IPAs can support people with disabilities [26]. One diary study with 19 users found they were largely satisfied with their Alexa interactions [13], while an interview study with 14 users found that IPAs did not behave as users expected them to; the lack of system feedback made it difficult for these users to refine their mental models of how IPAs worked [15].

This uncertainty about how IPAs function raises clear implications for privacy and security, since these devices rely on collecting and processing potentially sensitive data from users in a private setting (i.e., their home). Dorai et al. [8] conducted a forensic analysis to extract data and infer user information from a smart home system involving

[1] In this paper, we refer to interactions with IPAs embedded within a smartphone (e.g., Siri) as Phone IPA use and interactions with a standalone smart home device (e.g., Amazon Echo) as Home IPA use.

IPAs. Likewise, Chung and Lee [4] analyzed four months of data from an Alexa user and inferred patterns about the person's schedule, interests, and location. In a separate analysis, Chung et al. [3] identified four ways malicious actors could put IPA users' privacy and security at risk, including wiretapping, exploiting security vulnerabilities, impersonating a user, or eavesdropping on unintentional recordings.

Researchers are beginning to explore how IPA users evaluate privacy and security threats. One study found that only 2% of online product reviews for IPAs referenced privacy and security [12]. Those that did focused on the amount and type of data IPAs collect as well as its "creepiness" [12]. Zeng et al. [35] interviewed 15 smart home users, many of whom also used IPAs, and found that those with less sophisticated mental models of their smart home systems did not perceive many security threats. In addition, most respondents did not express privacy concerns; their reasons included not feeling personally targeted, trusting companies or governments who may access IPA data, or feeling satisfied their existing strategies to mitigate threats [35].

Only four of Pradhan et al.'s [26] 16 respondents discussed IPA security concerns, but half expressed privacy concerns about the "always on" nature of IPAs and their collection of personal data. Nearly one-third avoided certain IPA tasks or turned off the device at certain times. Social contexts also influence IPA use; for example, Moorthy and Vu [21] found that smartphone users were hesitant to use a mobile IPA for a task that involved private information—even more so if they were in a public location. This work highlights that privacy and security considerations draw on a complex interplay of technical operations, users' experiences and mental models, and contextual cues. However, most research only considers experiences of people who already use IPAs. In this study, we provide perspectives of non-users as well as users.

2.2 Applying Social Contract Approach to IPA Privacy

A growing body of scholarship argues that privacy is contextual in nature, and that protecting privacy depends on maintaining appropriate information flows between actors within a given context [16, 22, 23, 29]. Martin [16] notes that contextually dependent approaches to privacy mirror a contractual approach to norms, where privacy evolves as a social contract—a mutually beneficial agreement within a contracting community about how information is used and shared. Privacy as social contract implies that (1) online privacy expectations should depend on the context of the exchange, (2) users do not relinquish information without an expectation about how that information will be used within that context, and (3) companies that derive benefits from users, consumers, and employees disclosing information have an obligation to respect the privacy norms within their community [17].

The social contract framework suggests that information is governed by the norms of a contracting community, a self-described group of people with shared tasks, values, or goals and who are capable of establishing norms of ethical behavior for themselves [7]. Although contractors have the moral free space to develop authentic and legitimate privacy norms and expectations, privacy violations occur when "information is tracked, disseminated, or used against the agreement of the actors within the community through a breach of microsocial contracts" (p. 558) [17]. Through the lens of social contract theory, IPA users and IPA service providers form a contracting community. Both acting as the recipient and disseminator of information, they have a right and an obligation to abide by the privacy norms associated with IPA use. Empirically, respondents within a particular contracting community have a better understanding of the privacy norms than outsiders [16]. From this perspective, existing IPA users might hold different privacy attitudes compared to non-users. Similarly, we might expect one's level of trust in company compliance with social norms regarding data privacy and security to vary.

2.3 Technology Adoption and the Role of Privacy

Frameworks for understanding technology acceptance explain how users come to adopt and use a specific technology [19]. The Technology Acceptance Model (TAM) and its extensions inform the current study's exploration of the factors that affect IPA use. According to the original model [5], users' attitudes toward technology use determine their behavioral intentions, which directly influence the individuals' final use or rejection of the technology. In TAM, attitudes toward technology use are influenced by two personal beliefs: perceived ease of use and perceived usefulness. However, TAM falls short in recognizing how external contextual factors inform technology acceptance [1]. In response, the Unified Theory of Acceptance and Use of Technology (UTAUT) [31] suggests that three key constructs drive behavioral intentions to use the technology: *performance expectancy* (the perceived usefulness of the system), *effort expectancy* (the perceived ease of use), and *social influence* (to what degree an individual perceives that important others believe he or she should use the system). Additionally, *facilitating condition*, influences only the final decision to use or reject the technology [30]. Researchers have further extended the model by incorporating the constructs of *hedonic motivation* (i.e., fun or pleasure derived from the technology use), *price value* (consumers' cognitive tradeoff between the perceived benefits and the monetary cost), and *experience* and *habit* [30] to examine use of various technologies, including mobile health services [10] and social media [6].

In recent years, researchers have increasingly considered how privacy and security affects technology acceptance and use. For instance, Miltgen et al. [19] examined end-user acceptance of biometric-based identification systems and found that users who expressed higher data privacy concerns were more likely to perceive the technology as risky—and consequently, they were less likely to use the technology. However, as the current generation of IPAs is a relatively new technology for most consumers, research is just beginning to explore consumer attitudes toward IPAs. This study provides an opportunity to apply and extend technology acceptance frameworks by investigating privacy and trust as determinants of IPA acceptance and use.

3 Method

In January 2018, authors at two universities each invited a random sample of 3000 university staff to participate in a 10-15 minute online survey on technology use, with an opportunity to win one of five US$50 Amazon gift cards from a random drawing. The study was part of a larger project examining privacy attitudes and behaviors among adult smartphone users; therefore, participation was limited to smartphone owners 18 or older. At the close of the survey, 1178 people had completed the survey. The research team removed 18 cases for not meeting participation criteria or significant missing data, for a final sample size of 1160. Across the full sample, 59% of respondents were women, and 92% had obtained at least a bachelor's degree; respondents were generally young (*M*=38.17, *SD*=12.72, range: 20-82), with most (61.5%) owning an iPhone, compared with 37.8% owning an Android.

3.1 Measures and Variables

IPA Data Concerns and Data Confidence. We used an original, 7-item scale to measure privacy and security concerns associated with IPA device use (IPA Data Concerns; M=3.12, SD=1.14, α=.91). Responses were recorded on a five-point Likert scale from 1 (Not at All Concerned) to 5 (Extremely Concerned). Example statements include: "I am concerned that the device is always listening" and "I am concerned that other people might activate/access the device and trigger unauthorized purchases."

To measure respondents' trust of companies' compliance with the IPA social contract (i.e., that their use of IPAs are private, safe, and secure), we included an original, 4-item scale (IPA Data Confidence; M=1.94, SD=.86, α=.84). Responses were recorded on a five-point Likert scale from 1 (Not at All Confident) to 5 (Very Confident). Example statements are: "I'm confident information communicated between the device and the service provider is always encrypted" and "I'm confident that microphones on these devices are not activated without a user's direct action."

General Privacy and Mobile Data Concerns. General privacy concerns were measured by an 11-item scale [32] evaluating the level of concern respondents have in association with their use of communication technologies. Sample prompts include: "Private messages becoming public available" and "Your picture being used in a social media app." Respondents selected from a five-point Likert scale from 1 (Not at all concerned) to 5 (Very concerned) (M=3.27, SD= .97, α= .93).

Respondents' mobile data concerns were measured through an 8-item scale [34] asking, "How much do you agree or disagree with the following statements about your use of mobile phone apps." Sample statements include: "I believe that the location of my mobile device is monitored at least part of the time" and "I am concerned that mobile apps are collecting too much information about me." Respondents chose along a five-point Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree) (M=3.93, SD=.77, α= .93).

Digital Literacy Related to Smartphone Use. To measure users' digital literacy related to their smartphone use (*M*=4.16, *SD*=.83, α=.89), we asked respondents to indicate how confident they felt performing eight tasks on a smartphone. Example tasks include: "Adjusting which apps have permission to access my microphone," and "Creating a personal hotspot with my phone." Respondents responded along a five-point Likert scale from 1 (Not at All Confident) to 5 (Very Confident).

Experience Related to Phone IPA Use and Non-Use. We asked respondents if they had Siri, Google Assistant, or another IPA activated on their smartphones: 524 (45%) were current Phone IPA users, while 332 (28%) never used IPAs on their phones. An additional 128 (11%) reported they had used it in the past, but no longer used it, and 127 (11%) had disabled the feature. We also asked follow-up questions on use or non-use based on their response to this question.

Experience Related to Home IPA Use and Non-Use. We also asked respondents whether they owned a Home IPA device. Twenty-nine percent (n=319) reported that they owned at least one Home IPA device. Among this subgroup of Home IPA users, 227 (71%) owned an Amazon Echo or Echo Dot, while 92 (29%) reported owning a Google Home or Home Mini, and 39 (12%) owned both Home IPAs. We asked users to provide more information on their motivations for getting a device, and we asked non-users follow-up questions on whether they intended to purchase one in the future.

Control Variables. Our respondents provided basic demographic information, including their sex, current age, annual income, and education. We also asked questions about their knowledge of smartphone data sharing and, when applicable, tasks they performed with a Phone IPA. For the analyses presented below, we exclude education because the dataset is heavily skewed toward those with college degrees.

4 Findings

4.1 RQ1: Exploring Reasons for IPAs Use and Non-use

Motivations for IPA Adoption. For the 652 respondents who had ever used a Phone IPA—including those who currently used it and those who had used it in the past—we asked them to identify why they used it. The survey included a list of 11 possible reasons, (plus an open-ended option), and respondents could select multiple responses. The most popular reasons for using a Phone IPA were: (1) asking factual questions (82%); (2) getting directions/location of a place (65%); (3) asking silly/funny questions just for laughs (60%); (4) dictating a text message or email (51%); (5) setting a timer (47%). Additional responses that garnered fewer votes included asking advice, asking health-specific questions, and home automation.

For the 380 respondents who reported owning a Google Home or Amazon Alexa, we asked them to list their motivations for purchasing the device. Nearly half (47%) said they had received the IPA as a gift; others said they had purchased the device primarily to control smart home devices (13%), out of curiosity or for fun (12%), to stream music (10%), and to have hands-free access to online information (8%).

Barriers to IPA Adoption. For the 457 respondents who said they did not currently use a Phone IPA—including those who had never used it and those who had deactivated IPA features on their phone—we asked them to rate factors that may have played a role in their decision. They responded on a five-point Likert scale (1=Not at All Important to 5=Very Important). The factors most often cited by these respondents reflected concerns about utility, design, and privacy. They included: I don't see any benefits from this feature (*M*=3.48, *SD*=1.23); I don't like talking aloud to my phone (*M*=3.38, *SD*=1.36); the user interface is frustrating (*M*=3.18, *SD*=1.03); it's awkward to use (*M*=3.14, *SD*=1.03); it doesn't understand my voice most of the time (*M*=2.96, *SD*=1.34); and I have privacy/security concerns about these features (*M*=2.88, *SD*=1.37).

In addition, 425 Phone IPA non-users provided open-ended responses to the question, "What is the main reason you don't use or stopped using your phone's IPA?" The vast majority of responses reflected classical constructs in TAM and UTAUT, with many revealing low performance expectancy (i.e., low perceived usefulness) associated with IPA use. A second cluster of responses suggested a high effort expectancy (i.e., low perceived ease of use) associated with IPA use. For example, one respondent said, "*I find it more time consuming compared to just doing the task myself.*" Finally, social influence played a role in respondents' decision not to use IPA, with one respondent noting, "*I use my phone in places where silence is of utmost importance and I, therefore, do not talk directly to personal assistants.*"

Only 28 respondents (7%) identified privacy concerns and trust issues as their primary reason for not using Phone IPAs. For instance, one respondent said, "*I do not want my phone listening to every word I have to say during the day. I do not trust Siri or Google not to store information it hears while in listening mode.*" Another respondent expressed heightened concerns about the privacy of voice data: "*How do I know my voice patterns being stored for future use? Inflections are just as identifiable as other human characteristics.*" Other respondents feared "*the app listening all the time*" and felt their privacy would be "*compromised*" or "*invaded.*"

4.2 RQ2: Predicting Adoption and Use of IPAs

To explore differences among people who use and do not use IPAs, we built binary logistic regression models to predict IPA adoption. Table 1 summarizes the statistics for the final models predicting use of Phone and Home IPA devices, respectively. Predictors included background/demographic variables, privacy and security concerns, and experience with other types of IPAs.

Results from Model 1 (predicting Phone IPA adoption) indicated a significant

Table 1. Predicting adoption and use of Phone and Home IPAs

	Model 1 **Use of Phone IPA**	**Model 2** **Use of Home IPA**
	Parameter Estimates: Beta (Odds Ratio)	
Background		
Sex (Male)	-.23 (.79)	.00 (1.00)
Age	.02 (1.02)***	-.00 (.99)
Income	-.00 (1.00)	.11 (1.12)**
Smartphone digital literacy	.59 (1.77)***	.24 (1.24)*
Smartphone type (iPhone)	.45 (1.58)***	-.03 (.98)
Privacy and Security		
General privacy concerns	-.18 (.83)*	.01 (1.02)
Mobile privacy concerns	.02 (1.02)	.35 (1.41))**
IPA data concerns	-.07 (.93)	-.49 (.61)***
IPA data confidence	.31 (1.36)***	.27 (1.31)*
Experience with IPA		
Home IPA use (Yes)	.54 (1.58)***	–
Phone IPA use (Yes)	–	.54 (1.72)***
Model fit|	**χ2=141.0, df=11*****	**χ2=117.98, df=11*****
Nagelkerke Pseudo R^2	**.16**	**.14**

*p<.05, **p<.01, ***p<.001

correlation between Phone IPA use and age, smartphone digital literacy, the type of smartphone used, general privacy concerns, IPA data confidence, and using a Home IPA ($\chi^2(11)=141.0$, $p<.001$). Specifically, respondents who used their phone's IPA were more likely to be older but have a higher level of digital literacy related to smartphone use. They were also more likely to use an iPhone compared to an Android device. Phone IPA users reported a lower level of general privacy concerns and greater confidence in how data from their IPA was used. Finally, they were likely to also use a Home IPA device. Model 2 (predicting Home IPA adoption) revealed a significant association between Home IPA use and income, smartphone digital literacy, mobile privacy concerns, IPA data concerns, IPA data confidence, and having used Phone IPA ($\chi^2(11)=117.98$, $p<.001$). Compared with those who did not own a Home IPA, respondents who used Home IPAs reported higher income, grater smartphone skills, and more mobile privacy concerns. Home IPA users were also more likely to have a higher IPA data confidence, paired with a lower level of IPA data concerns. They were more likely to have used their phone's IPA as well.

4.3 RQ3: Explaining Behavioral Intention to Adopt Home IPA Devices

Table 2. Explaining behavioral intention to adopt Home IPA devices

	Intention to Adopt Home IPA Devices	
Reference category: Adamant (I'm confident I won't be purchasing one)	Ambivalent (I might or might not buy one)	Likely-converted (I'll probably purchase one in the next year)
	Parameter Estimates: Beta (Odds Ratio)	
Background factors		
Sex: Male	-.05 (.95)	.81 (2.24)*
Age	.01 (1.01)	.00 (1.00)
Smartphone digital literacy	.22 (1.24)*	.49 (1.64)*
Privacy attitudes		
General Privacy Concerns	.37 (1.45)***	.53 (1.69)*
Mobile Data Concerns	-.26 (.77)	- .03 (.98)
IPA-specific factors		
Don't use Phone IPA	-.68 (.51)***	-2.06 (.13)***
IPA data concerns	-.24 (.79) **	- .22 (.81)
IPA data confidence	.52 (1.67)***	.76 (2.14)***
Model fit: χ^2 = 147.75, df=14, p<0.001 | Nagelkerke Pseudo R^2 = .20		

*p<.05, **p<.01, ***p<.001

To answer RQ3, we built a multinomial logistic regression model to explore individual differences across non-users' (N=816) behavioral intentions to adopt Home IPAs in the future. The dependent variable was measured through respondents' response to the question, "How likely are you to buy a Home IPA device in the future?" Respondents had three options: "I'm confident I won't be purchasing one" (Adamant; 52.1%); "I might or might not buy one" (Ambivalent; 41.4%); and "I'll probably purchase one in the next year" (Likely-converted; 6.5%). In the final model, the reference category is "Adamant non-adopters" who stated they had no intention of purchasing a Home IPA. Table 2 summarizes the multinomial regression results.

In evaluating Home IPA non-users' likelihood of purchasing a device in the future, we found a number of factors predicted their intentions. Compared to those who were adamant they will not purchase a Home IPA, those who were more ambivalent or leaning toward purchasing a device had significantly higher smartphone digital literacy and higher general privacy concerns. These respondents were also more likely to currently use a Phone IPA than those who said they had no intention of buying a Home IPA. When compared to the ambivalent and likely-converted, those who had no plans to purchase a Home IPA had significantly higher concerns about how IPA-generated data might be used and significantly less confidence that data generated by IPAs is sufficiently secure and protected.

5 Discussion

In this paper, we considered users' perceived motivations and barriers to adopting IPA devices, which are popular both on smartphones and as standalone home devices. IPAs can be integrated into existing smart home ecosystems, which can include smart speakers, thermostats, lighting, home security, and more. As IPAs are a relatively new technology, this study sought to understand how consumers make decisions to use these devices (or not), and to consider how concerns about privacy and trust influence their decisions. For Phone IPAs users, the convenience these tools provide—especially in allowing for personalized, hands-free information-seeking and task completion—was very appealing. Users of Phone IPAs like Siri or Google Assistant were more likely to be older and have a higher level of smartphone digital literacy. They also reported both a lower level of general privacy concerns and greater confidence in how data from their IPA was used. These findings paint a picture of a Phone IPA user who is technologically literate and confident in how IPA providers manage their data.

For Home IPA users, nearly half of respondents reported receiving the device as a gift. This suggests that some users might not have considered issues of privacy and trust before deciding to allow an IPA into their home. Home IPA users tended to use their devices for tasks other than personalized services or information seeking, such as streaming music or controlling other smart devices. This data suggests that users of Home IPAs relate to these devices as novel additions—often via gifts—to their home, and rely on them for more basic functions compared to Phone IPA users. The increased mobile privacy concerns among Home IPA users might contribute to the lack of more personalized usage within the home, such as linking the device to their Amazon account to enable voice-activated purchasing.

Overall, IPA users tended to report lower levels of general privacy concerns, while also reporting high confidence that IPA providers ensured their use of such devices was private, safe, and secure. From a social contract theory perspective, this suggests users trust IPA service providers (Google, Amazon, and Apple) to abide by the anticipated norms of information flow and assure consumer data privacy and security.

The social contract framework also informs our findings for non-users. While reasons for not using IPAs ranged across many factors (e.g., lack of need, minimal perceived usefulness, and price), we highlight the role of privacy in non-adoption of IPAs. While only 7% of respondents articulated privacy concerns as the primary reason for not using IPAs, our analysis of intentions to adopt them in the future reveals a more complex story. Respondents who were adamant in their refusal to consider purchasing a Home IPA, for example, had significantly higher concerns about how IPA data might be used and significantly less confidence that data generated by IPAs is sufficiently secure. Those who were ambivalent or considering a purchase within the next year exhibited greater trust, mirroring existing users. This suggests that perceptions of whether IPA providers abide by the social contract around data privacy and security influence one's likelihood to adopt Home IPAs.

Overall, we see various aspects of the TAM and UTAUT adoption frameworks in respondents' decisions to adopt—or reject—IPAs. Issues of perceived usefulness, expected performance, and the effort to make such devices perform as expected influenced adoption decisions. More notably, respondents' attitudes towards IPAs were rooted in their trust—or lack thereof—that the IPA provider adhered to the implicit social contract about maintaining private and secure information flows appropriate to the use of such devices.

6 Limitations, Future Work, and Conclusion

Some limitations to this research must be noted. While we took steps to reach a diverse set of respondents through our sampling method, we were constrained to university employees, leading to a highly educated sample. Therefore, results may not generalize to the wider population of American adults. Furthermore, results were based on a one-time survey and therefore provide a snapshot of a particular moment in time. Because of this, we can only identify correlations between variables and not establish causation.

The results from this study reveal a complex picture of IPA users and non-users. Users of IPAs tend to trust that providers adhere to a social contract about the flow and usage of their information, yet privacy concerns differ between Phone and Home IPA users. Additional research can further examine these differences and potentially highlight whether users approach these different contexts of IPA usage with different sets of privacy expectations.

Our analysis of non-users' behavioral intentions to purchase an IPA in the future reveals the importance of trust within the social contract between users and IPA providers. Thus, IPA providers should note that not only does meeting consumer privacy expectations increase consumers' likelihood to adopt such devices [2, 11], but meeting consumer privacy expectations also increases overall trust in the company [18]. Conversely, violating privacy expectations inevitably leads to adverse consumer reactions, including non-adoption or rejection of a tool or service [20].

Future researchers should take a more inductive approach to identify consumers' privacy expectations. Understanding the factors that drive mutually beneficial and sustainable privacy norms is also important for IPA service providers to best meet the privacy expectations of consumers and maintain the social contract proven essential for continued adoption of such devices. Providing a fuller understanding of the contextual expectations of privacy and security within the IPA ecosystem can enhance the future design of these smart devices and related IoT technologies.

Acknowledgements

This publication is based upon work supported by the National Science Foundation under grants No 1640640 and 1640697.

References

1. Bagozzi, R.P.: The legacy of the technology acceptance model and a proposal for a paradigm shift. J. Assoc. Inf. Syst. 8, 4, 3 (2007).
2. Cases, A.-S. et al.: Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. J. Bus. Res. 63, 9–10, 993–999 (2010).
3. Chung, H. et al.: Digital forensic approaches for Amazon Alexa ecosystem. Digit. Investig. 22, S15–S25 (2017).
4. Chung, H., Lee, S.: Intelligent virtual assistant knows your life. CoRRabs/1803.00466 (2018).
5. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 319–340 (1989).
6. Doleck, T. et al.: Examining the antecedents of social networking sites use among CEGEP students. Educ. Inf. Technol. 22, 5, 2103–2123 (2017).
7. Donaldson, T., Dunfee, T.W.: Ties that bind: A social contracts approach to business ethics. Harvard Business School Press, Boston (1999).
8. Dorai, G. et al.: I know what you did last summer: Your smart home Internet of Things and your iPhone forensically ratting you out. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. pp. 49:1–49:10 ACM, New York, NY, USA (2018).
9. Druga, S. et al.: "Hey Google is it OK if I eat you?": Initial explorations in child-agent interaction. In: Proceedings of the 2017 Conference on Interaction Design and Children. pp. 595–600 ACM, New York, NY, USA (2017).
10. Dwivedi, Y.K. et al.: A generalised adoption model for services: A cross-country comparison of mobile health (m-health). Gov. Inf. Q. 33, 1, 174–187 (2016).
11. Eastlick, M.A. et al.: Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. J. Bus. Res. 59, 8, 877–886 (2006).
12. Fruchter, N., Liccardi, I.: Consumer attitudes towards privacy and security in home assistants. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. pp. LBW0501–LBW0506 ACM, New York, NY, USA (2018).
13. Lopatovska, I. et al.: Talk to me: Exploring user interactions with the Amazon Alexa. J. Librariansh. Inf. Sci. pp.1–14 (2018).
14. Lopatovska, I., Williams, H.: Personification of the Amazon Alexa: BFF or a Mindless Companion. In: Proceedings of the 2018 Conference on Human Information Interaction & Retrieval. pp. 265–268 ACM Press, New Brunswick, NJ, USA (2018).
15. Luger, E., Sellen, A.: "Like Having a Really Bad PA": The Gulf Between User Expectation and Experience of Conversational Agents. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 5286–5297 ACM, New York, NY, USA (2016).
16. Martin, K.E.: Diminished or just different?: A factorial vignette study of privacy as a social contract. J. Bus. Ethics. 111, 4, 519–539 (2012).
17. Martin, K.E.: Understanding privacy online: Development of a social contract approach to privacy. J. Bus. Ethics. 137, 3, 551–569 (2015).
18. McCole, P. et al.: Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. J. Bus. Res. 63, 9, 1018–1024 (2010).

19. Miltgen, C. et al.: Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context. Decis. Support Syst. 56, 103–114 (2013).
20. Miyazaki, A.D.: Perceived ethicality of insurance claim fraud: Do higher deductibles lead to lower ethical standards? J. Bus. Ethics. 87, 4, 589–598 (2008).
21. Moorthy, A.E., Vu, K.-P.L.: Privacy concerns for use of voice activated personal assistant in the public space. Int. J. Human–Computer Interact. 31, 4, 307–335 (2015).
22. Nissenbaum, H.: Privacy as contextual integrity. Wash. Law Rev. 79, 119–157 (2004).
23. Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life. Stanford Law Books, Stanford, Calif (2010).
24. Olmstead, K.: Nearly half of Americans use digital voice assistants, mostly on their smartphones, http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/ (2017).
25. Porcheron, M. et al.: “Do Animals Have Accents?”: Talking with Agents in Multi-Party Conversation. In: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. pp. 207–219 ACM, New York, NY, USA (2017).
26. Pradhan, A. et al.: “Accessibility came by accident”: Use of voice-controlled Intelligent Personal Assistants by people with disabilities. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 459:1–459:13 ACM, New York, NY, USA (2018).
27. Purington, A. et al.: “Alexa is my new BFF”: Social roles, user satisfaction, and Personification of the Amazon Echo. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. pp. 2853–2859 ACM, New York, NY, USA (2017).
28. Shoot, B.: St. Louis University Installs Amazon Echo Dots Campus-Wide, http://fortune.com/2018/08/15/amazon-alexa-echo-back-to-school-dorm-room/ (2018).
29. Stutzman, F., Hartzog, W.: Obscurity by design: An approach to building privacy into social media. In: Workshop on Reconciling Privacy with Social Media. ACM (2012).
30. Venkatesh, V. et al.: Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Q. 36, 1, 157–178 (2012).
31. Venkatesh, V. et al.: User acceptance of information technology: Toward a unified view. MIS Q. 425–478 (2003).
32. Vitak, Jessica: A digital path to happiness? In: Handbook of Media Use and Well-Being. Reinecke L, Oliver MB (eds) Routledge (2016).
33. Welch, C.: Amazon made a special version of Alexa for hotels that put Echo speakers in their rooms, https://www.theverge.com/2018/6/19/17476688/amazon-alexa-for-hospitality-announced-hotels-echo (2018).
34. Xu, H. et al.: Measuring mobile users’ concerns for information privacy. In: Proceedings of the International Conference on Information Systems 2012 on Digital Innovation in the Service Economy. pp. 1–16 (2012).
35. Zeng, E. et al.: End user security and privacy concerns with smart homes. In: Symposium on Usable Privacy and Security (SOUPS ’17). pp. 65–80 (2017).