Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers

Eugene Cho
Penn State University
University Park, PA, USA
exc75@psu.edu

S. Shyam Sundar
Penn State University
University Park, PA, USA
sss12@psu.edu

Saeed Abdullah
Penn State University
University Park, PA, USA
saeed@psu.edu

Nasim Motalebi
Penn State University
University Park, PA, USA
nfm5140@ist.psu.edu

ABSTRACT

"Always-on" smart speakers have raised privacy and security concerns, to address which vendors have introduced customizable privacy settings. But, does the act of customizing one's privacy preferences have any effects on user experience and trust? To address this question, we developed an app for Amazon Alexa and conducted a user study (N = 90). Our data show that the affordance to customize privacy settings enhances trust and usability for regular users, while it has adverse effects on power users. In addition, only enabling privacy-setting customization without allowing content customization negatively affects trust among users with higher privacy concerns. When they can customize both content and privacy settings, user trust is highest. That is, while privacy customization may cause reactance among power users, allowing privacy-concerned individuals to simultaneously customize content can help to alleviate the resultant negative effect on trust. These findings have implications for designing more privacy-sensitive and trustworthy smart speakers.

Author Keywords

Customization, privacy concern, power usage, security; smart speaker(s), voice assistant(s)

CSS Concepts

• Human computer interaction (HCI)~User studies • Security and privacy~Usability in security and privacy

INTRODUCTION

While a fast-growing number of people are adopting smart assistants, whether it be Alexa, Google Assistant or Siri, recently reported incidents are making users start to question if they can fully trust these virtual assistants with their data. If you ask Alexa if she listens to you all the time, she insists: "I only record and send audio back to the Amazon cloud when you say the wake word." However, that does not guarantee security of the storage and use of audio data retrieved by smart speakers. For instance, multiple mishaps have been reported with Alexa sending private conversations to an acquaintance and mishearing wake words [13,36]. Audio recordings from Alexa were also reported to be used to solve a murder case [33], which set an Arkansas man free, but showed how privacy rights could be compromised for legal reasons. To make the matter worse, major smart speaker producers, including Apple, Amazon and Google, were found to employ contractors to review users' voice recordings including sensitive information (e.g., confidential medical history, private conversations) for the purpose of quality control [15,46]. At this point, the mere fact that smart speakers have to be "always on", eavesdropping and transmitting audio data to the cloud, to work properly is enough to trigger privacy and security concerns among users.

In response to such concerns, Amazon recently added two new features. Through the Alexa mobile app, users can now review their voice interaction history and delete any recordings that occurred in the past. Users are also offered a choice to enable the "deletion by voice feature," and if they do, user utterances can be immediately rendered "off the record" by issuing simple voice commands such as "Alexa, delete what I just said" and "Alexa, delete everything I said today." On the one hand, providing an opportunity to delete their voice recordings can empower users, leading to some relief from unwanted data sharing. For instance, making privacy information more salient [44] and offering more control over the use of personal information for personalized content [45] have been shown to induce positive behavioral outcomes in web-based interactions. On the other hand, there also exists a possibility that users would not buy into such features to fully eliminate privacy issues [25], and simply consider them as a part of Amazon's public relations effort. If so, implementation of those features may only serve to remind users of privacy issues (i.e., negative priming effects) [5,20]. Especially, considering that smart speakers need to constantly gather audio data to operate properly and offer better user-tailored services, voice deletions may only elevate tension between security concerns and convenience provided by personalized online services [43].

In addition to adjusting privacy settings, there is much more that could be customized in smart speakers. For instance, users can enable and disable various Alexa skills (just like gadgets) through the Alexa app and the amazon.com site. For

CHI 2020, April 25–30, 2020, Honolulu, HI, USA.
 ACM ISBN 978-1-4503-6708-0/20/04...$15.00.
DOI: https://doi.org/10.1145/3313831.XXXXXXX
*update the above block and DOI per your rightsreview confirmation (provided after acceptance)

some applications (e.g., flash brief), users are allowed to choose particular information domains (e.g., politics, entertainment) and sources (e.g., NBC, Fox). Ways to summon information from smart speakers (e.g., wake words, skill name) can also be altered. Allowing users to customize content and interface in web-based interactions was found to improve user experience by affording users more agency [41]. Thus, it is worth exploring whether such customization, even when it is irrelevant to privacy, can also affect user trust with smart speakers. If positive effects of customization come from heightened user agency through the "act" of customization, regardless of the type of features or content customized, both adjusting privacy settings and content may have similar effects on user trust and experience. Moreover, if adjusting privacy settings only ends up creating negative privacy priming effects, general content customization may have more positive effects on user outcomes.

Yet, even if offering those customization options may enhance user experience, we cannot expect the effects of privacy and content customization to be identical to all users. The act of customization does demand extra time and cognitive effort, and some would not mind such costs for benefits in return, while others may consider it as too much effort. Especially, individual differences related to privacy and new technology usage patterns will be crucial in determining the adoption of smart speakers and the features offered by them. From their diary- and interview-based study, Lau, Zimmerman, and Schaub [25] found that current users of smart speakers based their adoption on factors such as convenience and early-adopter identity, whereas privacy concerns affected non-users. Similarly, even among users, the adoption of privacy customization features can differ by individual's judgment of the tension between privacy and convenience of personalized offerings.

In order to address these possibilities and answer all the questions raised above, we designed a study to empirically test if the effects of customizing (1) privacy setting in particular and (2) content in general can, independently and/ or (3) in combination, contribute to enhancing user experience and trust. Furthermore, we examined if individual differences in (4) privacy concerns and (5) power usage can alter the effects of customization, if any. Lastly, focused on actual user behaviors in customization, we explored if those personality traits, i.e., (6) privacy concerns and (7) power usage, predict certain user choices in customization (e.g., deletion of voice recordings, choice of particular sources).

CUSTOMIZATION EFFECTS ON TRUST

Some previous work on web-based customization of content and interface points to its general positive effects. According to the Modality-Agency-Interactivity-Navigability (MAIN) model [40], even the mere presence of customization features can have a positive effect on credibility perceptions of the media platform and content. Such effects occur through cueing of certain cognitive heuristics in users' mind (for example, by cueing the rule of thumb that 'more control is better'). That is, presence of interface features can affect our content perceptions even when they are external to the content. This is especially relevant in the domain of privacy settings for smart speakers, which are often adjusted after the interaction, since voice recordings have to be gathered first for users to receive content, and can be deleted later upon user discretion. Therefore, while privacy customization may not seem to directly influence the content users receive, letting them know that they can always modify and adjust privacy settings can be a strong psychological cue that affects user perceptions toward smart speakers and the content they deliver.

Will the generally positive cue effects of customization on user agency and control, suggested by the MAIN model [40], extend to particular customization features focused on privacy with voice-assistant technologies? When it comes to privacy with voice interactions, previous findings from relevant literature seem to convey conflicting messages. On the bright side, recent work on voice agents informs us that tracking and storing of the audio recordings is a major element that stirs up privacy-related concerns over smart speaker usage [10,30], and due to that, users value more control over deletion of those recordings [16]. In particular, adding UI features to delete audio data has been found to enhance control in data management and decrease intrusiveness with an audio sampling mobile app [16], and if those features can be enabled by voice in smart speakers, there is a possibility that they can further enhance user experience by facilitating hands-free interactions [10]. Studies in web-based interactions have also documented the positive effects from privacy assurance cues. For instance, Zhang and Sundar [49] found that presenting privacy customization features on a website, either in the form of simply showing the possibility of privacy adjustments or allowing users to actually opt in for privacy protection, decreased privacy concerns among users through heightened sense of control. In addition, displaying privacy policy more clearly and accessible in e-commerce [44] and social media [45] seem to enhance user engagement and positive attitudes.

However, weighing the benefits and costs of privacy control is not that simple. A study on a crowdfunding platform found that the effects of privacy control can go both ways [5]. Specifically, when users were given control over display of personal information, they showed increased engagement with the platform, but decreased their contributions from heightened awareness of potential privacy risks. John et al. [20] also demonstrated that scrutinizing individuals with sensitive questions reduced personal information sharing by priming them to consider the danger in disclosure. Such findings reflect the concept of "control paradox" in online privacy proposed by Brandimarte et al. [3] when they discovered how privacy-protective measures intended to offer more control paradoxically ended up making users feel more vulnerable through more information disclosure. Such findings suggest that while privacy customization may offer more control among users, it can also prime them about the

privacy pitfalls of using smart speakers. Especially, if users do not acknowledge the utility of smart speakers [25] or online privacy tools [39], due to reasons such as ineffective interface or inherent mistrust toward the service provider, privacy-protective voice features might not serve its purpose. In fact, many smart speaker adopters do not utilize privacy controls even though they are aware of those features, with some willing to trade privacy for convenience [25,30]. Due to competing pieces of theoretical evidence, we suggest our first research question to explore the effects of privacy customization as follows (*RQ1*). In particular, we focused on the customization effects on two dimensions of trust—source credibility (i.e., trust toward smart speaker as a source) and message credibility (i.e., trust toward content delivered by the smart speaker)—as well as security perceptions, and general user experience.

RQ1. Will customizing privacy setting have an effect on (a) user trust toward the smart speaker, (b) perceived credibility of content offered by the smart speaker, (c) perceived security and (d) usability of the smart speaker application?

Extending the MAIN model [40], the theory of interactive media effects (TIME) [41] suggests that there is another way for customization, beyond "cue" effects, to have an influence on user attitudes toward media and content, and that is by way of "action." When users engage in the activity of customizing the media content, such action can improve credibility evaluations through imbuing a sense of agency to users. For instance, in the context of web interaction, it was found that customizing widgets on web pages leads users to feel more in control of the web interaction [31], and customizing content categories (e.g., bookmarks, news clipper) for a web portal increases positive attitudes toward the website [21]. When applied to smart speakers, we can predict that active engagement in tailoring of content (for example, enabling particular skills or choosing preferred information sources) can positively affect how users view smart speakers and the content delivered by them. If this hypothesized positive effect derives from the general sense of agency arising from the act of customization, it is possible that customizing general content can improve overall user experience, and even have spill-over effects on user perceptions related to privacy and security. For instance, it has been found that allowing users to specify content preferences enhanced users' willingness to adopt a recommendation agent by increasing trust [24]. Relevant to this point, web content with higher relevance to users was found to offset negative impact of privacy concerns (triggered by the absence of privacy policy or security seals) on behavioral intention to use the web service [28].

On the other hand, we still have to contend with the fact that customizing content requires effortful action on the users' side. That is, the positive effects of customization can only be realized when users can justify all the effort they put into customization. For instance, Kang and Sundar [22] found that customization results in greater depletion of inner resources when individuals customized the web account for others (vs. themselves). Especially, if customization does not seem to offer clear individual benefit of protecting privacy, but instead becomes another chore, customizing the smart speaker interaction that is irrelevant to privacy may not affect enhance user trust and security perceptions. This led us to propose our second research question testing the content customization effects (*RQ2*). Due to the two-directional predictions for both privacy and content customization effects, we also explored the possibility of a trade-off or complementary effects between privacy and content customization (*RQ3*).

RQ2. Will customizing content have effect on (a) user trust toward the smart speaker, (b) perceived credibility of content offered by the smart speaker, (c) perceived security and (d) usability of the smart speaker application?

RQ3. Will the effects of privacy customization on (a) user trust toward the smart speaker, (b) perceived credibility of content offered by the smart speaker, (c) perceived security and (d) usability of the smart speaker application, change when users customize content irrelevant to privacy settings?

THE MODERATING ROLE OF PERSONALITY

Even if customization can be preferred by some individuals, it may not be favored by everyone. Some may not mind a little cognitive investment in customization to obtain what they want, others may think it is not worth going the extra mile. For privacy customization in particular, personal levels of inherent privacy and security concerns can make a difference. In fact, Westin [47] contrasts privacy fundamentalists (those who deeply care about their privacy rights) with privacy pragmatists (those who are willing to share information for potential benefits). If privacy customization seems to offer users more control, it may look more appealing to privacy fundamentalists than to privacy pragmatists. However, fundamentalists might also be more careful about evaluating the effectiveness of those privacy features before they fully trust them. Empirical findings also support the differential effects of information tailoring among individuals with different privacy attitudes. Those who experienced more privacy invasion before were found to express higher privacy concerns over personalization without explicit user consent [28,49]. Even when users openly customized (advergame) content, the positive customization effects on user attitudes were only seen among individuals with low privacy concerns, which the authors suspected that highly concerned users may have thought that "their customization preferences are being stored and used for marketing purposes" (p. 74) [48]. Yet, there are other pieces of evidence suggesting that customization can alleviate privacy concerns, especially as a counteracting force to the negative effects of automatic system-driven personalization techniques [49]. Thus, we suggest the following research question to explore if privacy concerns alter the effects of customization, and if so, in which direction.

RQ4. Will users' pre-existing privacy concerns alter the effects of (*i*) privacy and (*ii*) content customization on (a) user trust toward the smart speaker, (b) perceived credibility of content offered by the smart speaker, (c) perceived security and (d) usability of the smart speaker application?

In addition to privacy concerns, the most widely examined individual difference shown to have impact on information tailoring perceptions is power usage [6,31,42], which is an individual trait related to more efficient, competent, and motivated usage of new media technologies [32]. Due to the heightened sense of control provided by customization especially among power users [31], active customization serves to be a better option for power users than covert personalization when information privacy is not guaranteed [42]. Sensitivity to control among power users also suggests that personalization can increase user trust, but only when the information tailoring process by the system is not perceived as explicit to them [6]. In particular, Sundar and Marathe's [42] findings suggest that power users preferred customization (vs. personalization) when the website stated that it may use users' browsing information. However, when their data privacy was assured, users showed positive attitude changes for system-driven personalization. Applying such findings into the smart speaker context, it is possible that customizing content may be unnecessary to gain trust from power users, when they adjust privacy settings, whereas content customization may result in positive attitudes among non-power users, even with the absence of privacy customization. Thus, we aim to explore the moderating role of power usage in customizing privacy settings and content of smart speakers.

RQ5. Will the level of power usage alter the effects of (*i*) privacy and (*ii*) content customization on (a) user trust toward the smart speaker, (b) perceived credibility of content offered by the smart speaker, (c) perceived security and (d) usability of the smart speaker application?

CUSTOMIZATION CHOICES

Just as individual differences can have disparate effects on psychological outcomes derived from customization, they can also influence user choice in customization. Notwithstanding the various customization options offered to users, many simply interact with smart speakers on default settings, to avoid additional steps involved in customization (e.g., accessing the mobile smart speaker app and changing settings). It is also reported that users seldom use privacy controls, and complain that those features are not in alignment to their needs [25]. But if they were given a choice to delete voice history for privacy reasons over better personalized services, which option will they choose (*RQ6*)? It is possible that privacy fundamentalists who value data security [47], and non-power users who are less tech-savvy [32] and potentially less aware of technological benefits associated with retaining voice recordings, will opt for deleting (vs. saving) voice recordings when they adjust privacy settings. On the other hand, will individual differences influence content customization options, even when they are not related to privacy (*RQ7*)? To address the above questions of the specific choices users make when it comes to privacy setting and content customization, the following research questions are proposed.

RQ6. Will privacy concerns and power usage influence privacy customization choices?

RQ7. Will privacy concerns and power usage influence content customization choices?

METHOD

Participants

We recruited 90 participants from summer courses for extra credit at a large public university in the United States. The sample consisted of a larger portion of male (N = 51) and Caucasian (N = 75) students, but having those demographic characteristics (vs. their counterparts) did not alter the levels of the 4 major outcome variables (p > .16), which lessens the possibility of confounding gender and ethnicity effects. Admittedly, convenience sampling led us to have a particularly young sample (M_{Age} = 18.12, SD = 0.36), comprised of incoming 1st-year students. However, age is not considered a critical factor that would skew the results. For instance, a survey-based study with 310 respondents suggests that the effects of privacy concerns on attitudes toward smart home products is not significantly different between junior and senior groups [38]. In another survey with 305 participants, age showed a significant positive correlation with trust toward smart speakers, while no correlation with attitudes [8]. Yet, in the same study, age also seemed to increase intentions to adopt smart speakers [8].

Study Design

First, to examine if customizing privacy settings through smart speakers have an effect on user outcomes, approximately half the participants were randomly assigned to the privacy customization condition, and the other half, the control (i.e., no privacy customization) condition. Second, to test the effects of content customization, again about half of the sample was assigned to customize content, while the other half was not provided this affordance. This led us to adopt a 2 (privacy setting customization vs. control) X 2 (content customization vs. control) between-subjects experimental design, where participants were randomly assigned to one of the four conditions. For the smart speaker service, we used Alexa through the Amazon Echo device, considering its wide adoption, and a personified smart service [35].

Study Procedures

Upon arrival at the lab, participants received general information regarding the study procedure, and proceeded with the actual study after offering voluntary consent. Procedures involved interacting with a couple of Alexa applications and completing an online survey. The interaction session with Alexa started with activating a simple health Q&A application we developed for the purpose

of this study. The basic function of the application was to offer answers to 3 particular health-related questions that we guided participants to ask Alexa. The health-related questions and statements delivered by the application were related to topics of general interest but controversial in nature. No clear scientific evidence was provided with these statements. This was to induce an even distribution of message credibility perceptions among participants [18]. All participants asked the same 3 questions in order, and received identical responses from Alexa (Table 1).

Questions	Alexa Responses
Can medical Marijuana help people with addiction?	*The use of cannabis for addiction therapy is still debatable. Still, many argue that therapeutic marijuana can help people with alcohol or opioid dependencies by lowering tolerance and alleviating withdrawal symptoms.*
Should vaccines be required for children?	*All US states mandate 29 doses of 9 vaccines for children under 6. However, opponents caution that it may cause side effects, including seizures and paralysis. It is also argued that vaccines can cause problems like autism, ADHD, and diabetes.*
Is drinking milk healthy for us?	*The general belief is that vitamins and minerals in milk help strengthen our bones and improve cardiovascular health. However, many argue that milk contributes to obesity, allergies, stomach cancer, and other health issues.*

Table 1. Controversial health-related questions and statements.

However, when participants activated the health Q&A application, the setup session varied by the content customization vs. control conditions. In particular, when participants were assigned to the content customization condition, they went through one more task before posing the questions to Alexa. That is, they were asked to customize content (i.e., speech speed, content length, information source) before they were allowed to ask questions.

Afterwards, participants were asked to open another application that allowed users to delete voice recordings, only when they were assigned to the privacy customization condition. When users were assigned to customize both content and privacy settings, content customization was implemented prior to privacy customization, since users need some type of interaction with Alexa before they can delete their own voice recordings. As the last step, all participants completed an online questionnaire to share their thoughts about the interaction. See Table 2 for study procedures in each experimental condition.

Cond. / Steps	Control	Only Content Custom-ization	Only Privacy Custom-ization	Both
Open Health Q&A App	■	■	■	■
Customize Content		■		■
Ask 3 Health Qs & Get As	■	■	■	■
Open Privacy App.			■	■
Adjust Privacy Sett.			■	■

Table 2. Study procedures by experimental conditions.
Note: Shaded cells indicate steps taken by participants for each experimental condition. Cond. = conditions, Q = question, A = answer, App = application, Sett: settings.

Manipulated Conditions

For the content customization manipulation, two Alexa apps were developed, one that offered controversial health-related information without content customization options (named "Health Answers"), and the other with the customization options (named "My Health Facts"). Amazon does not allow identical names for different skills, and we had to create app names that were not too similar to avoid invoking the wrong skill. While both of the apps offered identical information, participants who were assigned to the content customization condition went through one more task before asking the questions to Alexa. In the content customization condition, after participants opened the app by saying "Alexa, open My Health Facts," Alexa asked if the users wanted to adjust the (1) speed of speech (i.e., "Welcome to Health Facts! Before we begin, would you like me to adjust the speed of my speech? Please choose one from slower or faster or the same."), (2) length of content (i.e.," Would you like to adjust the length of my health answers? Please choose one from abbreviated or regular."), and (3) primary source of information (i.e., Would you also choose your preferred primary source of health information? We have WebMD, Mayo Clinic, and GenieMD.").

Afterwards, if participants were assigned to the privacy setting customization condition, they were asked to open another privacy setting app labeled as "My Voice Settings", which asked if users wanted to (1) delete (or save) their most recent voice recording, and/or (2) automatically delete voice recordings on a monthly basis (or not). We opted for audio deletion as our privacy customization manipulation since it is similar to the feature that Amazon recently added in response to potential privacy issues, and also since clearing user history is a common privacy protection measure taken in other web-based platforms (e.g., Google automatic history deletion). It is also expected to cue illusion of control in that smart speakers require continuous retention of audio data in order to provide personalized content. In terms of the

distinction between deletion of recent vs. monthly recordings, albeit they are not completely mutually exclusive behaviors, we thought that the deletion of immediate (vs. monthly) data may reflect a more sensitive data protection behavior, and the reported distribution in the results section signals that they are indeed different behaviors. To note, before participants were asked if they want to delete voice recordings, they were reminded of the benefits or reasons of audio data retention, based on opening statements such as "Welcome to My Voice Settings! We keep voice recordings to improve the accuracy of the results provided to you," "Remember, deleting your voice recordings may degrade your experience using voice features. Would you still like to delete your most recent voice recordings?"

While we used custom-built skills for this study, to increase ecological validity, the skills were designed to give an impression that it was an Amazon-supported feature by using 1st person pronouns and the default Alexa voice throughout the interaction. Also, while there was some time difference in Alexa interaction across experimental conditions, we consider the more time and effort taken for customization to be part of the customization experience (a potential cost to obtain tailored information), as discussed earlier.

Measured Variables

User trust toward Alexa

Ten items from Koh and Sundar [23] that were designed to measure trust toward media technology (separate from media content) was modified to fit the context of this study. Example items include: "I believe that Alexa acted in my best interest," "Alexa was competent in providing the content I need. I would characterize Alexa as honest." (M = 5.75, SD = 0.17, α = .95).

Perceived content credibility

Thirteen items were borrowed from Appleman and Sundar's [1] scale developed to measure message credibility (i.e., Accurate, Authentic, Believable, Complete, Concise, Consistent, Well-presented, Objective, Representative, No Spin, Expert, Will have impact, Professional; M = 5.84, SD = 0.99, α = .95).

Perceived security

We revised 5 items from the perceived web security scale by Salisbury et al. [37] to measure participants' security perceptions regarding their interaction with Alexa, e.g., "Alexa will not misuse my personal information," "I feel secure sharing personal information with Alexa," "I feel safe about my interactions with Alexa." (M = 3.65, SD = 1.71, α = .93).

Perceived usability

We selected 12 items that fit the context of smart speakers from Lund's 30-item [29] USE scale, built to measure usefulness, satisfaction, and ease of use of a product or service. Sample items include: "It is user-friendly," "I don't notice any inconsistencies as I use it," "It works the way I want it to work." (M = 5.75, SD = 0.99, α = .92).

Privacy concerns

Three items were from Dinev and Hart [11] were used to measure individual's level of privacy concerns: "I am concerned about people I do not know obtaining personal information about me from my online activities," "I am concerned who might access my personal records electronically" (M = 5.21, SD = 1.41, α = .83).

Power usage (of technology)

Five items were selected from Marathe et al.'s [32] power usage scale: i.e., "Using any technological device comes easy to me," "I make good use of most of the features available in any technological device," "I feel like information technology is a part of my daily life," "Using information technology gives me greater control over my work environment," "I would feel lost without information technology" (M = 5.47, SD = 1.01, α = .73).

Usage level of Alexa and other smart speakers

We also asked how frequently they used both (a) Alexa, and (b) other virtual assistants such as Google Assistant, Siri, Cortana (1 = *Never*, 4 = *Regularly once a week*, 7 = *More than once a day*). Due to high correlation (r = .52, p < .001), we combined the two items by adding them (M = 5.99, SD = 3.39), instead of putting them separately in the same model, and included as a control variable in the main analyses.

RESULTS

For the main analyses, we built a set of regression models with interaction terms, including privacy setting customization, content customization, privacy concerns, and power usage, with mean-centered values for continuous variables, on all the four outcome variables (see Table 3). One outlier was identified who scored extremely low on trust toward both Alexa and content, and excluded in the models that had those variables as dependent variables. In addition, confirming that power usage is conceptually different from privacy concerns, the correlation between the two personality variables was non-significant (r = -.11, p = .28), allowing us to include them together in the same model without multicollinearity concerns. In order to avoid overfitting the model, we also ran another reduced model to secure at least more than 10 observations for each term (predictor) [2] on each dependent variable. To do so, we dropped the non-significant control variable (i.e., smart speaker usage frequency) and 2-way interaction term (i.e., privacy X content customization) that does not affect the soundness of the reduced models, as well as the two 3-way interaction terms. We note that all the (marginally) significant 2-way interaction effects found in the full model remained, or became significant in the reduced model (see values in parentheses in Table 3).

In terms of the main effects of personalities and previous experience with smart speakers, power usage tended to positively affect all the outcome variables (ps < .02), and those who used smart speakers more frequently tended to report higher perceived usability of the Alexa skill (b = 0.11, t = 1.91, p = .06). Interestingly, privacy concerns also

positively predicted trust toward Alexa (b = 0.20, t = 2.23, p = .02). Results of the main analyses testing the customization effects indicated that neither customizing privacy setting (*RQ1*) nor content (*RQ2*) showed significant main effects on any of the user outcomes: (a) trust toward Alexa (ps > .85), (b) content credibility (ps > .62), (c) security (ps > .73), and (d) usability (ps > .10). There were also no trade-offs or complementary effects between privacy and content customization (*RQ3*) on any of the 4 outcome variables (p > .41), when personality was not taken into account.

However, there appeared a marginally significant moderation effect of privacy concerns (*RQ4*) with content customization on perceived usability (b = 0.13, t = 1.85, p = .07; see row *RQ4ii* in Table 3). More interestingly, one significant three-way interaction emerged on content credibility (b = 0.15, t = 2.23, p = .03; *RQ3+4* in Table 3). Other than these, no other two-way or three-way interactions with privacy concerns were significant (ps = .30). When the two-way interaction were plotted, it showed that individuals who hold low privacy concerns evaluated the Alexa skill as more usable when they customized the content, whereas privacy-conscious users reported lower perceived usability when the content was customized, compared to the control condition (see Figure 1). The three-way interaction pattern revealed that privacy setting customization had positive effects on content trust among those with low privacy concerns, but negative effects among participants reporting high privacy concerns, but only when they did not customize content (see Figure 2). When users were allowed to customize content, the effects of privacy setting customization seemed to disappear.

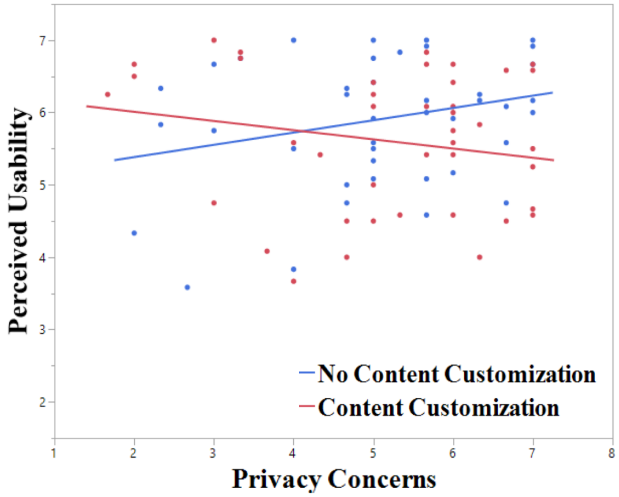

Figure 1. Interaction effects between content customization and privacy concerns on perceived usability.

DVs / IVs	(a) Trust Toward Alexa			(b) Content Credibility			(c) Perceived Security			(d) Perceived Usability		
	b	*t*	*p*	*b*	*t*	*p*	*b*	*t*	*p*	*b*	*t*	*p*
Smart Speaker Usage Frequency	0.01 (N/A)	0.35 (N/A)	.72 (N/A)	0.00 (N/A)	0.15 (N/A)	.88 (N/A)	0.05 (N/A)	1.00 (N/A)	.32 (N/A)	**0.05 (0.06)**	**1.91 (2.04)**	**.06 (.04)**
Privacy Customization (*RQ1*)	0.01 (0.01)	0.13 (0.05)	.90 (.96)	0.01 (-0.00)	0.14 (-0.14)	.89 (.89)	0.06 (0.05)	0.35 (0.26)	.73 (.80)	0.11 (0.10)	1.15 (1.07)	.26 (.29)
Content Customization (*RQ2*)	0.02 (0.01)	0.20 (0.08)	.85 (.94)	0.05 (0.04)	0.50 (0.47)	.62 (.64)	-0.10 (-0.10)	-0.34 (-0.38)	.73 (.71)	0.16 (0.16)	1.66 (1.73)	.10 (.09)
Privacy Concerns	**0.20 (0.20)**	**2.30 (2.45)**	**.02 (.02)**	0.11 (0.08)	1.55 (1.13)	.12 (.26)	-0.10 (-0.20)	-1.05 (-1.43)	.30 (.16)	0.08 (0.06)	1.05 (0.84)	.30 (.41)
Power Usage	**0.29 (0.27)**	**2.47 (2.42)**	**.02 (.02)**	**0.27 (0.26)**	**2.94 (2.81)**	**.004 (.01)**	**0.57 (0.58)**	**3.15 (3.35)**	**.002 (.001)**	**0.29 (0.28)**	**2.99 (2.93)**	**.003 (.004)**
Privacy X Content Customization (*RQ3*)	0.10 (N/A)	0.84 (N/A)	.41 (N/A)	0.04 (N/A)	0.38 (N/A)	.71 (N/A)	0.01 (N/A)	0.05 (N/A)	.96 (N/A)	0.03 (N/A)	0.33 (N/A)	.74 (N/A)
Privacy Customization X Privacy Concerns (*RQ4i*)	-0.10 (-0.10)	-0.87 (-0.93)	.39 (.35)	0.07 (0.08)	0.98 (1.10)	.33 (0.28)	-0.10 (-0.00)	-0.37 (-0.14)	.71 (.89)	0.02 (0.02)	0.28 (0.33)	.78 (.74)
Content Customization X Privacy Concerns (*RQ4ii*)	0.08 (0.09)	0.94 (1.16)	.35 (.25)	0.04 (0.08)	0.61 (1.24)	.54 (0.22)	0.04 (0.07)	0.31 (0.56)	.76 (58)	**0.13 (0.15)**	**1.85 (2.20)**	**.07 (.03)**
Privacy Customization X Power Usage (*RQ5i*)	**0.22 (0.23)**	**1.87 (2.03)**	**.07 (.046)**	0.14 (0.15)	1.55 (1.64)	.13 (0.11)	0.09 (0.13)	0.48 (0.73)	.63 (.46)	**0.21 (0.21)**	**2.18 (2.24)**	**.03 (.03)**
Content Customization X Power Usage (*RQ5ii*)	0.02 (0.04)	0.21 (0.37)	.84 (.72)	-0.10 (-0.00)	-0.60 (-0.38)	.55 (0.70)	-0.30 (-0.30)	-1.50 (-1.46)	.14 (.15)	-0.10 (-0.10)	-1.25 (-1.15)	.22 (.25)
Privacy X Content Custom. X Privacy Concerns (*RQ3+4*)	0.07 (N/A)	0.82 (N/A)	.41 (N/A)	**0.15** (N/A)	**2.23** (N/A)	**.03** (N/A)	0.13 (N/A)	1.00 (N/A)	.32 (N/A)	0.08 (N/A)	1.05 (N/A)	.30 (N/A)
Privacy X Content Custom. X Power Usage (*RQ3+5*)	-0.10 (N/A)	-0.46 (N/A)	.65 (N/A)	0.09 (N/A)	0.97 (N/A)	.33 (N/A)	0.05 (N/A)	0.29 (N/A)	.77 (N/A)	0.08 (N/A)	0.83 (N/A)	.41 (N/A)

Table 3. Regression model testing the main and interaction effects of customization, privacy concern, and power usage.
Note: Values in parentheses are from the reduced models. Effects in bold and underlined represent significant (p < .05) and marginally significant (p < .08) effects on the outcome variables.

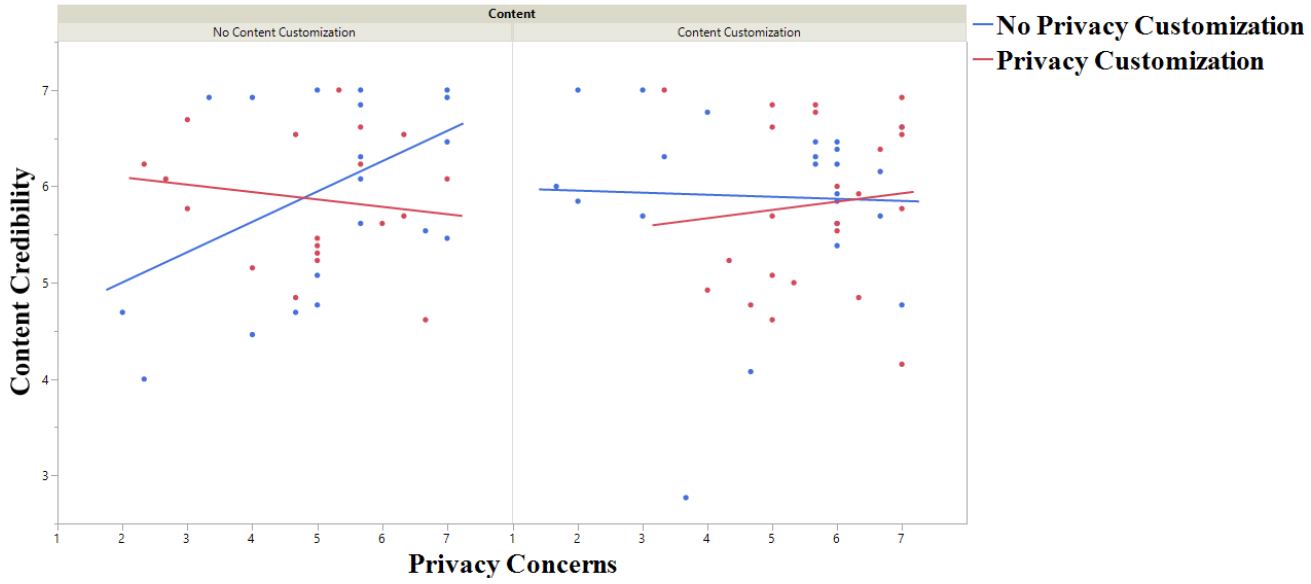

Figure 2. Interaction effects among privacy customization, content customization, and privacy concerns on content credibility.

Regarding the moderating effects of power usage (*RQ5*), a marginally significant interaction effect with privacy setting customization on trust toward Alexa ($b = 0.22$, $t = 1.87$, $p = .07$), and a significant moderation effect on perceived usability ($b = 0.21$, $t = 2.18$, $p = .03$) emerged (See row *RQ5i* in Table 3), with no other significant two- or three-way interaction effects ($p > .13$). When these interactions were decomposed, privacy setting customization (vs. control) seemed to exert positive effects on trust and usability, but only among non-power users, whereas for power users, the effects were reversed. Especially, when users did not customize privacy settings, power users seemed to trust Alexa more (see Figure 3), and rate the usability of the Alexa skill higher (see Figure 4), but such positive effects dissipated when they were asked to adjust privacy settings.

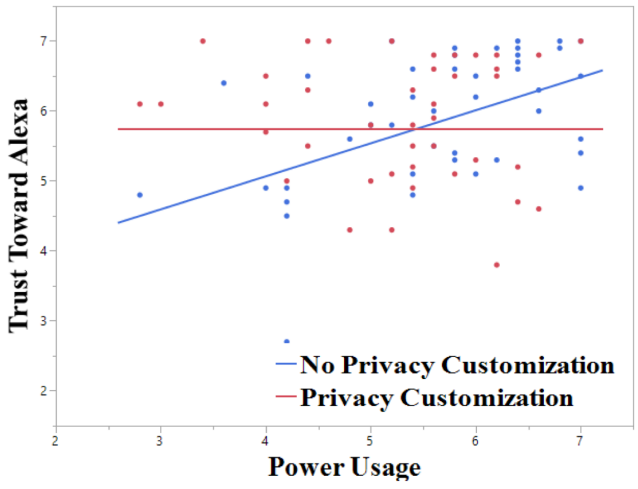

Figure 3. Interaction effects between privacy customization and power usage on trust toward Alexa.

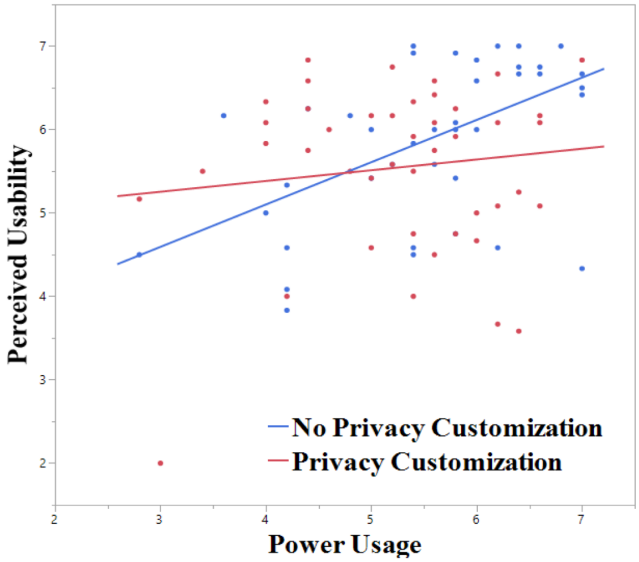

Figure 4. Interaction effects between privacy customization and power usage on perceived usability.

With regards to the customization choices (*RQ6-7*), first, privacy setting choices were distributed evenly. Among 45 participants assigned to the privacy setting customization, 23 chose to delete their most recent voice recordings, and 24 said they would like their voice recordings deleted on a monthly basis. Specifically, 13 chose to delete recent voice recordings as well as make deletion automatic on a monthly basis, whereas 11 left their most recent voice recordings to be saved without opting for monthly deletion. Ten participnts chose to only delete their recent voice recordings without adjusting monthly settings, and 11 only enabled monthly deletion but saved their most recent voice recordings. As predicted by *H2*, individual differences in personality seemed to have an effect on privacy setting choices,

especially for the most recent voice recordings. When a logistic regression was run on recent voice recording deletion choices, privacy concerns had a marginally significant positive effect (Exp(b) = 1.72, p = .07; M_{Save} = 4.98, SD_{Save} = 1.33; M_{Delete} = 5.71, SD_{Delete} = 1.04), and power usage had a marginally significant negative effect (Exp(b) = 0.49, p = .07; M_{Save} = 5.57, SD_{Save} = 0.88; M_{Delete} = 5.00, SD_{Delete} = 0.99) on user action to delete rather than save their recent voice recordings. However, privacy concerns (Exp(b) = 1.18, p = .52) and power usage (Exp(b) = 1.16, p = .64) did not affect deletion of voice recordings on a monthly basis. On the other hand, the 46 users who were assigned to the content customization condition seemed to choose the default option or the first option offered. Majority chose regular speed (regular = 42, fast = 1, slow = 1), normal length (normal = 33, abbreviated = 11), and WebMD as their primary source (WebMD = 33, Mayo Clinic = 12, GenieMD = 1). Directly connected to *RQ4*, when logistic regressions were run on content length and source choices, personality traits did not show any significant effects on content customization choices (ps > .34). Taking into consideration the significant personality effects on recent voice recordings deletion, we further explored if the choice users made further affected user outcomes. However, t-tests showed that even when privacy-concerned users deleted (vs. saved) their voice history, the action did not have effects on any of the four outcome variables (ps > .22).

In sum, the analyses yielded three major findings. First, power users seemed to report higher trust and usability perceptions toward Alexa, but only in the absence of privacy customization. When they were offered the option to adjust privacy settings, such positive effects among power users disappeared. Second, among privacy-conscious individuals, privacy customization lowered content credibility; however, when the option to customize content was offered in addition to privacy settings, content credibility was unaffected even among users with high privacy concerns. This was the case even when content customization in general degraded user experience among privacy-concerned users. Third, privacy-concerned users and non-power users were more likely to delete than save their most recent voice recordings when offered the choice. Despite such action taken, however, deletion did not result in better or worse user outcomes.

DISCUSSION

Theoretical and Practical Implications

Our findings suggest that the presence of privacy customization cancels out the positive effects of smart-speaker interaction on user experience and trust, rather than enhancing agency among users. For power users, the negative effects pertained to the smart speaker service (i.e., smart agent, and the smart speaker skill), and for privacy-conscious users, it was the credibility of content offered by the smart agent. Power users' decreased trust toward Alexa with privacy customization signaled the control paradox [3], potentially arising from negative priming effects [5,20]. In terms of diminished usability reported among power users, adding privacy customization may have been perceived as extra work without clear benefits. Considering that power users tend to save their voice recordings when given a choice to delete them, it is likely that they clearly acknowledge the benefits associated with collection of their data, such as getting personalized content, thereby making privacy customization a rather pointless and time-consuming process. For users with high privacy concerns, the negative privacy customization effects appeared on content credibility, but only without content customization. When they customized content in addition to privacy settings, it seemed to defuse the negative priming effect of privacy customization. By informing users that they can actively set the tone of the content they will receive, the privacy customization app ceased to be seen as a threat on content credibility. Still, the added cognitive investment involved in content customization seemed to decrease the usability of the smart speaker app.

Overall, such findings offer privacy implications to interactions with not only smart speakers specifically, but also inform the development of more trustworthy and user-friendly voice-enabled privacy-sensitive technologies in general. Similar to the case of smart speakers [25], smart home environments in general [4], and other speech-initiated systems such as smart driving [12] stir up security concerns and trust issues stemming from lack of user control in interface design and data management. Furthermore, it difficult to apply standard security solutions to those smart systems due to their heightened connectivity as well as resource-constrained nature [27]. According to the interactivity effects model in TIME [41], customization can be one effective interactive feature to enhance credibility perceptions toward systems by fostering user engagement through "action". For instance, Hanus and Fox [14] found that users were more likely to be moved by persuasive messages coming from an embodied speech agent, when they customized (vs. watch customization of) the appearance of that virtual agent. However, it seems customization specifically tied to privacy in voice interactions needs a more careful approach to build trust and enhance usability among users. Inherently, smart speakers require retention and accumulation of audio data to enhance performance and even operate in a basic level, which makes the conflict between privacy and convenience inevitable [25,30]. To make matters worse, recent data management controversies involving technology giants (e.g., Facebook–Cambridge Analytica data scandal) complicate the trust relationship between users and service providers, and increase doubt in the companies' data management abilities [25,30]. Thus, refined privacy controls that balance the tension between privacy and convenience, as well as stronger security assurance from smart speaker companies, are needed to regain user trust and enhance user experience.

Based on the above theoretical implications suggested by the study findings, we propose design guidelines as follows.

First, considering the cognitive cost of privacy customization in user experience, the customization feature and process should be designed to be more user-friendly, and seamlessly integrated into the human-to-smart speaker interaction. Especially, "cueing" customization can be a powerful and less effortful way for users to realize the benefits, and overcome the price, of privacy customization. For instance, Zhang and Sundar [49] found that even the mere presence of privacy customization interface cues (without actual action taken) led to similar outcomes to personally adjusting privacy settings. Thus, smart speakers can be designed to provide privacy assurances up front, but offer customization options for only those who actually prefer it. Second, the complementary effects of content customization to privacy concerns (on content credibility), and general tension between security and convenience, discovered in our study points to enhancing compatibility of different types of customization/personalization techniques. For instance, designers can develop privacy tools that incorporates some type of content customization, or embed simple agency-enhancing features in personalized services (e.g., apply personalization only with user initiation or explicit consent; reactive/overt personalization rather than proactive/covert personalization [6,49]). Third, significant moderating effects of personality inform us that designers should consider developing adaptive systems to cater to individual factors and modality preferences. In fact, Hoegen et al. [17] found that conversational voice agents that adapt to gradually match users' particular conversational style (i.e., empathic and considerate interaction style) were evaluated to be more trustworthy by users. In addition, individual's level of privacy concerns also affected modality preference in smart speaker interactions, in that users having less concerns over privacy expressed more connection to smart speakers with voice over text interactions [7]. This suggests that customization options and processes should be designed to be more flexible and adaptable to individual differences regarding their level of privacy concerns and smart speaker usage behaviors. In sum, when offering privacy customization in particular, service providers should make an extra effort to reassure users, especially power users and privacy concerned individuals, about privacy being an important concern in designing and offering services, and offer various customizable features that are seamlessly and adaptively integrated to the system.

Limitation and Suggestions

While this study adds to recent research on the topic of smart speakers and privacy, mostly focused on investigating general user thoughts on privacy and security (e.g., [9,25]), by testing the effects of actual privacy measures taken by users in a controlled environment, some limitations of this study merit note. To begin with, generalizability issues and confounding factors stem from the study design. Even with arguments offered in the methods section, we acknowledge the low representativeness of our young, and mostly Caucasian, college sample. Also, utilizing custom-built skills that only responded to pre-designed scripts left little flexibility to the users, in stark contrast to real-life settings, not to mention that custom-built apps are more subject to system failures (e.g., four students repeatedly said "yes" before asking all questions, which led to repetition of the opening comment). Furthermore, while we conceptualized and operationalized time spent in using customization features as part of the customization experience, admittedly, longer interaction time among individuals assigned to customization conditions may have influenced usability (e.g., impressed by voice-based interactive customization feature) and credibility and privacy (e.g., extended audio data collection) perceptions. In addition, while we selectively chose measures to represent general credibility and usability perceptions, adoption of more comprehensive and widely adopted scales (e.g., User Experience Questionnaire; UEQ [26]), tailored to smart interactive systems (e.g., trust in automated systems [19,34]), could have made the findings more generalizable as well as specialized to the context of study. Lastly, we understand that this study could have been complemented by gathering qualitative insights from users to offer more concrete explanations on why certain decisions were made. It is recommended that future research take into account these methodological issues as well as adopt a mixed-method approach to enhance generalizability of the study findings.

CONCLUSION

Despite its intention, offering customization options for privacy settings seemed to invoke a sense of loss in control and efficiency among tech-savvy power users. Yet, allowing users to put specific requests regarding how they want their content was found to resolve the potential negative effects of privacy priming among privacy-conscious individuals. Informed by such findings, designers and service providers should consider incorporating various content customization options to lower mistrust in content and relieve user concerns over privacy. Furthermore, we expect integration of positive security assurance cues and seamless privacy customization processes in voice interaction to be key in enhancing user experience with smart speakers.

REFERENCES

[1] Alyssa Appelman and S. Shyam Sundar. 2016. Measuring message credibility: Construction and validation of an exclusive scale. *Journalism & Mass Communication Quarterly* 93, 1: 59–79. https://doi.org/10.1177/1077699015606057

[2] Michael A. Babyak. 2004. What you see may not be what you get: A brief, nontechnical introduction to overfitting in regression-type models. *Psychosomatic Medicine* 66, 3: 411–421. https://doi.org/10.1097/01.psy.0000127692.23278.a9

[3] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4, 3: 340–347. https://doi.org/10.1177/1948550612455931

[4] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *Proceedings of the 2016 European Intelligence and Security Informatics Conference*, 172–175. https://doi.org/10.1109/EISIC.2016.21

[5] Gordon Burtch, Anindya Ghose, and Sunil Wattal. 2015. The hidden cost of accommodating crowdfunder privacy preferences: A randomized field experiment. *Management Science* 61, 5: 949–962. https://doi.org/10.1287/mnsc.2014.2069

[6] Tsai-Wei Chen and S. Shyam Sundar. 2018. This app would like to use your current location to better serve you: Importance of user assent and system transparency in personalized mobile services. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3174111

[7] Eugene Cho. 2019. Hey Google, can I ask you something in private? In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–9. https://doi.org/10.1145/3290605.3300488

[8] Lei Chu. 2019. *Why would I adopt a smart speaker? : Consumers' intention to adopt smart speakers in smart home environment* (Master's Thesis). University of Twente. Retrieved from https://essay.utwente.nl/77187/

[9] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. "Alexa, can I trust you?" *Computer* 50, 9: 100–104. https://doi.org/10.1109/MC.2017.3571053

[10] Benjamin R. Cowan, Nadia Pantidi, David Coyle, Kellie Morrissey, Peter Clarke, Sara Al-Shehri, David Earley, and Natasha Bandeira. 2017. "What can i help you with?": infrequent users' experiences of intelligent personal assistants. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services - MobileHCI '17*, 1–12. https://doi.org/10.1145/3098279.3098539

[11] Tamara Dinev and Paul Hart. 2005. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce* 10, 2: 7–29. https://doi.org/10.2753/JEC1086-4415100201

[12] Anna-Katharina Frison, Philipp Wintersberger, Amelie Oberhofer, and Andreas Riener. 2019. ATHENA: supporting UX of conditionally automated driving with natural language reliability displays. In *Proceedings of the 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications Adjunct Proceedings - AutomotiveUI '19*, 187–193. https://doi.org/10.1145/3349263.3351312

[13] Dennis Green. 2018. Here's how the Alexa spying scandal could become Amazon's worst nightmare. *Business Insider*. Retrieved from https://www.businessinsider.com/amazon-alexa-spying-scandal-creates-trust-problem-with-customers-2018-5

[14] Michael D. Hanus and Jesse Fox. 2015. Persuasive avatars: The effects of customizing a virtual salesperson's appearance on brand liking and purchase intentions. *International Journal of Human-Computer Studies* 84: 33–40. https://doi.org/10.1016/j.ijhcs.2015.07.004

[15] Alex Hern. 2019. Apple contractors "regularly hear confidential details" on Siri recordings. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

[16] Alexis Hiniker, Jon E. Froehlich, Mingrui Zhang, and Erin Beneteau. 2019. Anchored audio sampling: A seamless method for exploring children's thoughts during deployment studies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–13. https://doi.org/10.1145/3290605.3300238

[17] Rens Hoegen, Deepali Aneja, Daniel McDuff, and Mary Czerwinski. 2019. An end-to-end conversational style matching agent. In *Proceedings of the 19th ACM International Conference on Intelligent Virtual Agents - IVA '19*, 111–118. https://doi.org/10.1145/3308532.3329473

[18] Carl I. Hovland and Walter Weiss. 1951. The influence of source credibility on communication effectiveness. *Public Opinion Quarterly* 15, 4: 635–650. https://doi.org/10.1086/266350

[19] Jiun-Yin Jian, Ann M. Bisantz, and Colin G. Drury. 2000. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics* 4, 1: 53–71. https://doi.org/10.1207/S15327566IJCE0401_04

[20] Leslie K. John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research* 37, 5: 858–873. https://doi.org/10.1086/656423

[21] Sriram Kalyanaraman and S. Shyam Sundar. 2006. The psychological appeal of personalized content in web portals: Does customization affect attitudes and behavior? *Journal of Communication* 56, 1: 110–132. https://doi.org/10.1111/j.1460-2466.2006.00006.x

[22] Hyunjin Kang and S. Shyam Sundar. 2013. Depleted egos and affirmed selves: The two faces of customization. *Computers in Human Behavior* 29, 6: 2273–2280. https://doi.org/10.1016/j.chb.2013.05.018

[23] Yoon Jeon Koh and S. Shyam Sundar. 2010. Effects of specialization in computers, web sites, and web agents on e-commerce trust. *International Journal of Human-Computer Studies* 68, 12: 899–912. https://doi.org/10.1016/j.ijhcs.2010.08.002

[24] Sherrie Y. X. Komiak and Izak Benbasat. 2006. The effects of personalization and familiarity on trust and

adoption of recommendation agents. *MIS Quarterly* 30, 4: 941–960. https://doi.org/10.2307/25148760

[25] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW: 1–31. https://doi.org/10.1145/3274371

[26] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *HCI and Usability for Education and Work*, Andreas Holzinger (ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[27] Changmin Lee, Luca Zappaterra, Kwanghee Choi, and Hyeong-Ah Choi. 2014. Securing smart home: Technologies, security challenges, and security requirements. In *2014 IEEE Conference on Communications and Network Security*, 67–72. https://doi.org/10.1109/CNS.2014.6997467

[28] Ting Li and Till Unger. 2012. Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems* 21, 6: 621–642. https://doi.org/10.1057/ejis.2012.13

[29] Arnold M. Lund. 2001. Measuring usability with the USE Questionnaire. *Usability Interface* 8, 2: 3–6. Retrieved from http://www.stcsig.org/usability/newsletter/index.html

[30] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4: 250–271. https://doi.org/10.2478/popets-2019-0068

[31] Sampada Marathe and S. Shyam Sundar. 2011. What drives customization?: control or identity? In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11*, 781–790. https://doi.org/10.1145/1978942.1979056

[32] Sampada Marathe, S. Shyam Sundar, Marije Nije Bijvank, Henriette Van Vugt, and Jolanda Veldhuis. 2007. Who are these power users anyway? Building a psychological profile. Retrieved from http://citation.allacademic.com/meta/p_mla_apa_research_citation/1/7/2/9/3/p172936_index.html

[33] Elliott C. McLaughlin. 2017. Suspect OKs Amazon to hand over Echo recordings in murder case. *CNN*. Retrieved from https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

[34] Stephanie M. Merritt, Heather Heimbaugh, Jennifer LaChapell, and Deborah Lee. 2013. I Trust it, but I don't know why: Effects of implicit attitudes toward automation on trust in an automated system. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 55, 3: 520–534. https://doi.org/10.1177/0018720812465081

[35] Amanda Purington, Jessie G. Taft, Shruti Sannon, Amanda Purington, Jessie G. Taft, Shruti Sannon, Natalya N. Bazarova, and Samuel Hardman Taylor. 2017. "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 - CHI EA '17*, 2853–2859. https://doi.org/10.1145/3027063.3053246

[36] Ethan Sacks. 2018. Alexa privacy fail highlights risks of smart speakers. *NBC news*. Retrieved from https://www.nbcnews.com/tech/innovation/alexa-privacy-fail-highlights-risks-smart-speakers-n877671

[37] W. David Salisbury, Rodney A. Pearson, Allison W. Pearson, and David W. Miller. 2001. Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems* 101, 4: 165–177. https://doi.org/10.1108/02635570110390071

[38] Jungwoo Shin, Yuri Park, and Daeho Lee. 2018. Who will be smart home users? An analysis of adoption and diffusion of smart homes. *Technological Forecasting and Social Change* 134: 246–253. https://doi.org/10.1016/j.techfore.2018.06.029

[39] Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. 2013. The post that wasn't: Exploring self-censorship on Facebook. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work - CSCW '13*, 793–802. https://doi.org/10.1145/2441776.2441865

[40] S. Shyam Sundar. 2009. The MAIN model: A heuristic approach to understanding technology effects on credibility. In *Digital media, youth, and credibility*. The MIT Press, Cambridge, MA, 72–100.

[41] S. Shyam Sundar, Haiyan Jia, T. Franklin Waddell, and Yan Huang. 2015. Toward a theory of interactive media effects (TIME): Four models for explaining how interface features affect user psychology. In *The Handbook of the Psychology of Communication Technology*. Wiley Blackwell, Malden, MA, 47–86.

[42] S. Shyam Sundar and Sampada S. Marathe. 2010. Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research* 36, 3: 298–322. https://doi.org/10.1111/j.1468-2958.2010.01377.x

[43] David G. Taylor, Donna F. Davis, and Ravi Jillapalli. 2009. Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research* 9, 3: 203–223. https://doi.org/10.1007/s10660-009-9036-2

[44] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22, 2: 254–268. https://doi.org/10.1287/isre.1090.0260

[45] Catherine E. Tucker. 2014. Social networks, personalized advertising, and privacy controls. *Journal*

of Marketing Research 51, 5: 546–562. https://doi.org/10.1509/jmr.10.0355

[46] James Vincent. 2019. Yep, human workers are listening to recordings from Google Assistant, too. *The Verge*. Retrieved from https://www.theverge.com/2019/7/11/20690020/google-assistant-home-human-contractors-listening-recordings-vrt-nws

[47] Alan Westin. 1967. *Privacy and Freedom*. New York: Atheneum.

[48] Verena M. Wottrich, Peeter W.J. Verlegh, and Edith G. Smit. 2017. The role of customization, brand trust, and privacy concerns in advergaming. *International Journal of Advertising* 36, 1: 60–81. https://doi.org/10.1080/02650487.2016.1186951

[49] Bo Zhang and S. Shyam Sundar. 2019. Proactive vs. reactive personalization: Can customization of privacy enhance user experience? *International Journal of Human-Computer Studies* 128: 86–99. https://doi.org/10.1016/j.ijhcs.2019.03.002