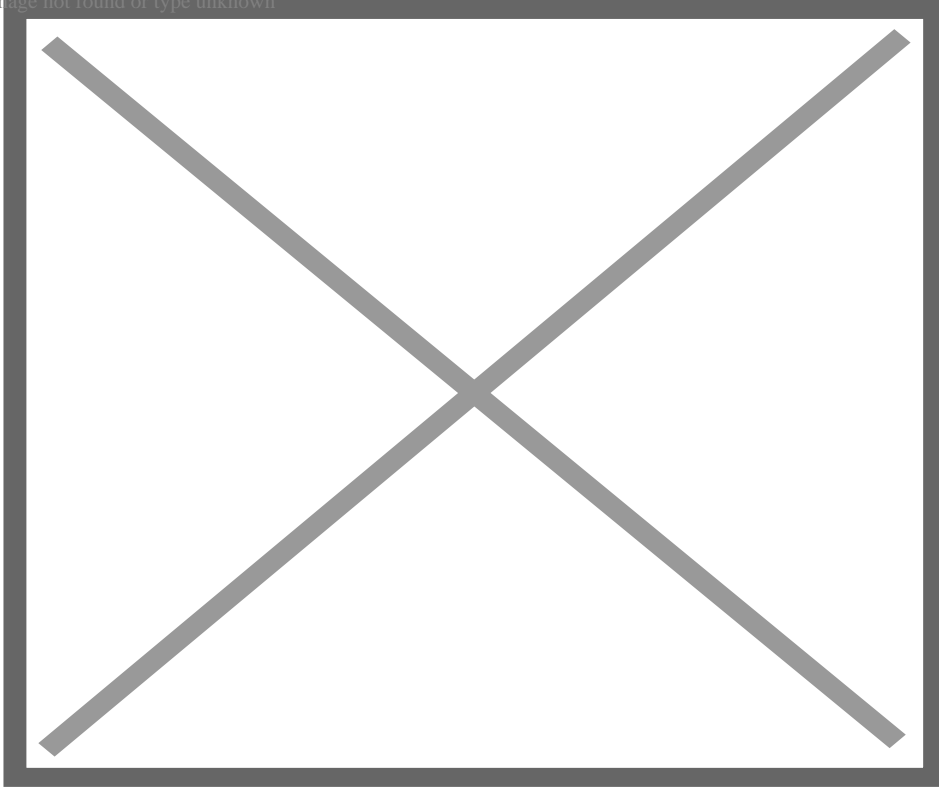


Alexa

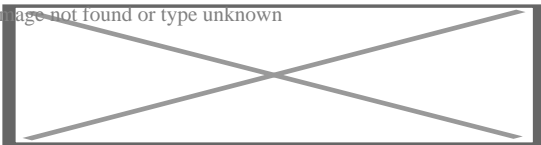
Description

No image found or type unknown



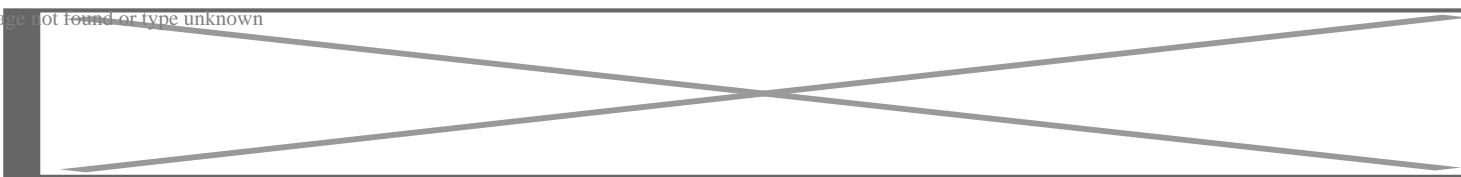
The [nothing to hide argument](#) states that individuals have no reason to fear or oppose surveillance programs unless they are afraid it will uncover their own illicit activities. An individual using this argument may claim that an average person should not worry about government surveillance, as they would have "nothing to hide".

No image found or type unknown



Edward Snowden aptly challenges this notion, stating, "*Saying, 'I don't care about privacy because I have nothing to hide,' is like saying, 'I don't care about freedom of speech because I have nothing to say.'*"

No image found or type unknown



[US20140337131A1](#)

See also: patents.google.com/patent/US20160259308A1/en (Smart-home automation system that suggests or automatically implements selected household policies based on sensed observations)



Further References

Sacks, E.. (2018). Alexa privacy fail highlights risks of smart speakers. NBC News

Show/hide publication abstract

“Alexa, can i trust you? the revelation that a woman in portland, oregon, had her private conversations secretly recorded by the voice-controlled amazon virtual devices in her home and then sent to a random contact in seattle has caused mounting concern about vulnerabilities behind the burgeoning technology of so-called smart speakers. the concern is warranted, said jennifer king, director of consumer privacy at the center for internet and society at stanford university, because this type of advanced technology is not fully understood by consumers. ‘we are basically testing fodder as they roll out more and more technologies that are based on artificial intelligence,’ king told nbc news. ‘these companies are crowdsourcing these algorithms. as a consumer, you’re basically helping them learn as they go.’”

Furey, E., & Blue, J.. (2018). Alexa, Emotions, Privacy and GDPR

Plain numerical DOI: 10.14236/ewic/hci2018.212

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“We exist in a world where emotional expression is a central facet of what makes us human. it allows us to interact richly with others and aids us in functioning as a society. affective computing, also known as artificial emotional intelligence is the area of study that seeks to enable the development of systems and devices with the capacity to understand and replicate these human affects. the race is on to develop intelligent computing systems that can mimic human interaction and also emulate and convince humans that they are human too, building a sense of trust. the amazon echo and its intelligent personal assistant, ‘alexa’, is currently one of the most popular and pervasive of these intelligent devices. the human name given to this technological entity alludes to its human-like conversation abilities. however, most adult humans would quickly establish that „alexa? is not a real person. this is obviously intimated through the automated voice, but is further demonstrated by a lack of recognition and display of any emotion. the advent of vcds like alexa raises a plethora of significant standard privacy considerations. this paper provides further speculation into the privacy concerns relating to the ability of these devices to gather data relating to an individual?s emotional state. this is conducted with consideration for the new general data protection regulation (gdpr) introduced in may,

2018.”

Mittal, M., & Manocha, S.. (2022). Alexa! Examine privacy perception and acceptance of voice-based artificial intelligence among digital natives. *Journal of Information and Optimization Sciences*

Plain numerical DOI: 10.1080/02522667.2022.2134367

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“The user has requested enhancement of the downloaded file.”

Combs, M., Hazelwood, C., & Joyce, R.. (2022). Are you listening? – an observational wake word privacy study. *Organizational Cybersecurity Journal: Practice, Process and People*

Plain numerical DOI: 10.1108/ocj-12-2021-0036

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Purpose digital voice assistants use wake word engines (wwe) to monitor surrounding audio for detection of the voice assistant’s name. there are two failed conditions for a wwe, false negative and false positive. wake word false positives threaten a loss of personal privacy because, upon activation, the digital assistant records audio to the voice cloud service for processing. design/methodology/approach this observational study attempted to identify which amazon alexa wake word and amazon echo smart speaker resulted in the fewest number of human voice false positives. during an eight-week period, false-positive data were collected from four different amazon echo smart speakers located in a small apartment with three female roommates. findings results from this study suggest the number of human voice false positives are related to wake word selection and amazon echo hardware. results from this observational study determined that the wake word alexa resulted in the fewest number of false positives. originality/value this study suggests amazon alexa users can better protect their privacy by selecting alexa as their wake word and selecting smart speakers with the highest number of microphones in the far-field array with 360-degree geometry.”

Xie, F., Zhang, Y., Yan, C., Li, S., Bu, L., Chen, K., ... Bai, G.. (2022). Scrutinizing Privacy Policy Compliance of Virtual Personal Assistant Apps. In *ACM International Conference Proceeding Series*

Plain numerical DOI: 10.1145/3551349.3560416

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“A large number of functionality-rich and easily accessible applications have become popular among various virtual personal assistant (vpa) services such as amazon alexa. vpa applications (or vpa apps for short) are accompanied by a privacy policy document that informs users of their data handling practices. these documents are usually lengthy and complex for users to comprehend, and developers

may intentionally or unintentionally fail to comply with them. in this work, we conduct the first systematic study on the privacy policy compliance issue of vpa apps. we develop skipper, which targets amazon alexa skills. it automatically depicts the skill into the declared privacy profile by analyzing their privacy policy documents with natural language processing (nlp) and machine learning techniques, and derives the behavioral privacy profile of the skill through a black-box testing. we conduct a large-scale analysis on all skills listed on alexa store, and find that a large number of skills suffer from the privacy policy noncompliance issues.”

Major, D., Huang, D. Y., Chetty, M., & Feamster, N.. (2022). Alexa, Who Am i Speaking To?: Understanding Users’ Ability to Identify Third-Party Apps on Amazon Alexa. ACM Transactions on Internet Technology

Plain numerical DOI: 10.1145/3446389

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Many internet of things devices have voice user interfaces. one of the most popular voice user interfaces is amazon’s alexa, which supports more than 50,000 third-party applications (‘skills’). we study how alexa’s integration of these skills may confuse users. our survey of 237 participants found that users do not understand that skills are often operated by third parties, that they often confuse third-party skills with native alexa functions, and that they are unaware of the functions that the native alexa system supports. surprisingly, users who interact with alexa more frequently are more likely to conclude that a third-party skill is a native alexa function. the potential for misunderstanding creates new security and privacy risks: attackers can develop third-party skills that operate without users’ knowledge or masquerade as native alexa functions. to mitigate this threat, we make design recommendations to help users better distinguish native functionality and third-party skills, including audio and visual indicators of native and third-party contexts, as well as a consistent design standard to help users learn what functions are and are not possible on alexa.”

Maccario, G., & Naldi, M.. (2023). Alexa, Is My Data Safe? The (Ir)relevance of Privacy in Smart Speakers Reviews. International Journal of Human-Computer Interaction

Plain numerical DOI: 10.1080/10447318.2022.2058780

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart speakers equipped with intelligent voice processing functions, like siri and amazon echo, have become widespread globally. however, their recording and networking capabilities spur concerns about users’ privacy. in this research, we report the results of a text-mining analysis of customers’ perception of privacy in smart speakers. the corpus comprises over 4,500 reviews of the echo line of smart speakers collected from amazon. smart speakers owners appear to be mostly oblivious to privacy issues since the fraction of those mentioning privacy in their reviews is largely below 3%. the average sentiment towards privacy is positive, though the average hides a significant fraction exhibiting a negative sentiment. however, those negative perceptions do not affect the overall sentiment polarity

towards the product, which stays positive.”

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K.. (2021). ‘Okay google, what about my privacy?’: User’s privacy perceptions and acceptance of voice based digital assistants. Computers in Human Behavior

Plain numerical DOI: 10.1016/j.chb.2021.106763

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Conversational artificial intelligence (ai) backed alexa, siri and google assistants are examples of voice-based digital assistants (vbda) that are ubiquitously occupying our living spaces. while they gather an enormous amount of personal information to provide bespoke user experience, they also evoke serious privacy concerns regarding the collection, use and storage of personal data of the consumers. the objective of this research is to examine the perception of the consumers towards the privacy concerns and in turn its influence on the adoption of vbda. we extend the celebrated utaut2 model with perceived privacy concerns, perceived privacy risk and perceived trust. with the assistance of survey data collected from tech-savvy respondents, we show that trust in technology and the service provider plays an important role in the adoption of vbda. in addition, we notice that consumers showcase a trade-off between privacy risks and benefits associated with vbda while adopting the vbda such technologies, reiterating their calculus behaviour. contrary to the extant literature, our results indicate that consumers’ perceived privacy risk does not influence adoption intention directly. it is mediated through perceived privacy concerns and consumers’ trust. then, we propose theoretical and managerial implications to conclude the paper.”

Loideain, N. N., & Adams, R.. (2020). From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments. Computer Law and Security Review

Plain numerical DOI: 10.1016/j.clsr.2019.105366

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“With female names, voices and characters, artificially intelligent virtual personal assistants such as alexa, cortana, and siri appear to be decisively gendered female. through an exploration of the various facets of gendering at play in the design of siri, alexa and cortana, we argue that this gendering of vpas as female may pose a societal harm, insofar as they reproduce normative assumptions about the role of women as submissive and secondary to men. in response, this article turns to examine the potential role and scope of data protection law as one possible solution to this problem. in particular, we examine the role of data privacy impact assessments that highlight the need to go beyond the data privacy paradigm, and require data controllers to consider and address the social impact of their products.”

Bianco, S., Celona, L., Ciocca, G., Marelli, D., Napoletano, P., Yu, S., & Schettini, R.. (2021). A smart mirror for emotion monitoring in home environments. *Sensors*

Plain numerical DOI: 10.3390/s21227453

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart mirrors are devices that can display any kind of information and can interact with the user using touch and voice commands. different kinds of smart mirrors exist: general purpose, medical, fashion, and other task specific ones. general purpose smart mirrors are suitable for home environments but the exiting ones offer similar, limited functionalities. in this paper, we present a general-purpose smart mirror that integrates several functionalities, standard and advanced, to support users in their everyday life. among the advanced functionalities are the capabilities of detecting a person’s emotions, the short- and long-term monitoring and analysis of the emotions, a double authentication protocol to preserve the privacy, and the integration of alexa skills to extend the applications of the smart mirrors. we exploit a deep learning technique to develop most of the smart functionalities. the effectiveness of the device is demonstrated by the performances of the implemented functionalities, and the evaluation in terms of its usability with real users.”

Chung, J., Bleich, M., Wheeler, D. C., Winship, J. M., McDowell, B., Baker, D., & Parsons, P.. (2021). Attitudes and Perceptions Toward Voice-Operated Smart Speakers Among Low-Income Senior Housing Residents: Comparison of Pre- and Post-Installation Surveys. *Gerontology and Geriatric Medicine*

Plain numerical DOI: 10.1177/23337214211005869

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart speakers have the potential to support independent living and wellness among low-income senior housing (lish) residents. the aim of this study was to examine and compare lish residents’ attitudes and perceptions toward smart speakers at two time points: before and after technology use (n = 47). a descriptive survey was administered to ask questions about hedonic motivation, perceived ease of use, self-efficacy, perceived usefulness of some potential or existing smart speaker features, cost, and privacy. participants were initially favorable toward using a smart speaker and its digital agent (e.g., alexa) as a daily assistant and wellness tool. they especially liked the smart speaker’s potential functionality of detecting harmful events and notifying someone to receive immediate help. the comparison of pre- and post-use responses revealed non-significant declines in most items, with the exception of willingness to use alexa as a reminder system (p <.01), asking alexa for help (p <.01), and asking for help in using alexa (p <.01). this finding may reflect confusion or frustration with the device among participants. we conclude with recommendations for the design of smart speakers specifically tailored to the needs of lish residents.”

Sweeney, M. E., & Davis, E.. (2020). Alexa, are you listening?: An exploration of smart voice assistant use and privacy in libraries. *Information Technology and Libraries*

Plain numerical DOI: 10.6017/ITAL.V39I4.12363

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart voice assistants have expanded from personal use in the home to applications in public services and educational spaces. the library and information science (lis) trade literature suggests that libraries are part of this trend, however there are few empirical studies that explore how libraries are implementing smart voice assistants in their services, and how these libraries are mitigating the potential patron data privacy issues posed by these technologies. this study fills this gap by reporting on the results of a national survey that documents how libraries are integrating voice assistant technologies (e.g., amazon echo, google home) into their services, programming, and checkout programs. the survey also surfaces some of the key privacy concerns of library workers in regard to implementing voice assistants in library services. we find that although voice assistant use might not be mainstreamed in library services in high numbers (yet), libraries are clearly experimenting with (and having internal conversations with their staff about) using these technologies. the responses to our survey indicate that library workers have many savvy privacy concerns about the use of voice assistants in library services that are critical to address in advance of library institutions riding the wave of emerging technology adoption. this research has important implications for developing library practices, policies, and education opportunities that place patron privacy as a central part of digital literacy in an information landscape characterized by ubiquitous smart surveillant technologies.”

Sun, K., Chen, C., & Zhang, X.. (2020). “alexa, stop spying on me!”: Speech privacy protection against voice assistants. In *SenSys 2020 – Proceedings of the 2020 18th ACM Conference on Embedded Networked Sensor Systems*

Plain numerical DOI: 10.1145/3384419.3430727

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Voice assistants (vas) are becoming highly popular recently as a general means of interacting with the internet of things. however, the use of always-on microphones on vas imposes a looming threat on users’ privacy. in this paper, we propose micshield, the first system that serves as a companion device to enforce privacy preservation on vas. micshield introduces a novel selective jamming mechanism, which obfuscates the user’s private speech while passing legitimate voice commands to the vas. it achieves this by using a phoneme level jamming control pipeline. our implementation and experiments demonstrate that micshield can effectively protect a user’s private speech, without affecting the va’s responsiveness.”

Neville, S. J.. (2021). The domestication of privacy-invasive technology on YouTube: Unboxing the Amazon Echo with the online warm expert. *Convergence*

Plain numerical DOI: 10.1177/1354856520970729

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“The purpose of this article is to explore how unboxing videos on youtube contribute to the domestication of privacy-invasive technology. further, the objective is to show how consumer influencers on youtube adapt to the flexible persona of the online warm expert (owe) which expands the concept of the ‘warm expert’ from the domestication literature (bakardjieva, 2005, internet society: the internet in everyday life. london: sage publications). i argue that the owe and unboxing discourse advance corporate interests of surveillance capitalism in home environments by promoting the circulation of emergent consumer technologies and eschewing meaningful discussion of privacy and surveillance issues. a case study of the amazon echo smart speaker and alexa, its voice-activated personal assistant, is presented. the research consists of a qualitative thematic analysis of unboxing videos (n = 73) and viewer comments on youtube. unboxing discourse reflects normative consumer culture values that are detached from critical discussions of surveillance or the informational privacy framework of end-user agreements. as a practical implication, the study helps look beyond the household and traditional social relationships in the domestic sphere to understand how technological domestication is being shaped in a paradigm of consumer culture that is fused with the infrastructural and cultural logics of the internet and social media.”

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J.. (2021). Privacy norms for smart home personal assistants. In Conference on Human Factors in Computing Systems – Proceedings

Plain numerical DOI: 10.1145/3411764.3445122

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart home personal assistants (spa) have a complex ecosystem that enables them to carry out various tasks on behalf of the user with just voice commands. spa capabilities are continually growing, with over a hundred thousand third-party skills in amazon alexa, covering several categories, from tasks within the home (e.g. managing smart devices) to tasks beyond the boundaries of the home (e.g. purchasing online, booking a ride). in the spa ecosystem, information flows through several entities including spa providers, third-party skills providers, providers of smart devices, other users and external parties. prior studies have not explored privacy norms in the spa ecosystem, i.e., the acceptability of these information flows. in this paper, we study privacy norms in spas based on contextual integrity through a large-scale study with 1,738 participants. we also study the influence that the contextual integrity parameters and personal factors have on the privacy norms. further, we identify the similarities in terms of the contextual integrity parameters of the privacy norms studied to distill more general privacy norms, which could be useful, for instance, to establish suitable privacy defaults in spa. we finally provide recommendations for spa and third-party skill providers based on the privacy norms studied.”

Fortunati, L., Edwards, A., Manganelli, A. M., Edwards, C., & de Luca, F.. (2022). Do People Perceive Alexa as Gendered? A Cross-Cultural Study of People’s Perceptions, Expectations, and Desires of Alexa

. Human-Machine Communication

Plain numerical DOI: 10.30658/hmc.5.3

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Mainly, the scholarly debate on alexa has focused on sexist/anti-woman gender representations in the everyday life of many families, on a cluster of themes such as privacy, insecurity, and trust, and on the world of education and health. this paper takes another stance and explores via online survey methodology how university student respondents in two countries (the united states, n = 333; and italy, n = 322) perceive alexa’s image and gender, what they expect from this voice-based assistant, and how they would like alexa to be. results of a free association exercise showed that alexa’s image was scarcely embodied or explicitly gendered. rather, alexa was associated with a distinct category of being- the vba, virtual assistant, or digital helper-with which one talks, and which possesses praiseworthy technical and social traits. expectations of alexa and desires regarding alexa’s ideal performance are presented and compared across the two country samples.”

Edu, J., Ferrer-Aran, X., Such, J., & Suarez-Tangil, G.. (2022). Measuring Alexa Skill Privacy Practices across Three Years. In WWW 2022 – Proceedings of the ACM Web Conference 2022

Plain numerical DOI: 10.1145/3485447.3512289

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart voice assistants are transforming the way users interact with technology. this transformation is mostly fostered by the proliferation of voice-driven applications (called skills) offered by third-party developers through an online market. we see how the number of skills has rocked in recent years, with the amazon alexa skill ecosystem growing from just 135 skills in early 2016 to about 125k skills in early 2021. along with the growth in skills, there is increasing concern over the risks that third-party skills pose to users’ privacy. in this paper, we perform a systematic and longitudinal measurement study of the alexa marketplace. we shed light on how this ecosystem evolves using data collected across three years between 2019 and 2021. we demystify developers’ data disclosure practices and present an overview of the third-party ecosystem. we see how the research community continuously contribute to the market’s sanitation, but the amazon vetting process still requires significant improvement. we perform a responsible disclosure process reporting 675 skills with privacy issues to both amazon and all affected developers, out of which 246 skills suffer from important issues (i.e., broken traceability). we see that 107 out of the 246 (43.5%) skills continue to display broken traceability almost one year after being reported. as a result, the overall state of affairs has improved in the ecosystem over the years. yet, newly submitted skills and unresolved known issues pose an endemic risk.”

Jonathan Leblang. (2018). Alexa Privacy and Data Handling Overview. Amazon Web Services

Show/hide publication abstract

“Getting privacy right takes careful attention, and amazon has built privacy deeply into the echo

hardware and alexa service, by design. this paper provides background and details of two areas of interest to alexa for business customers and users: when is audio streamed from an echo device to the alexa cloud, and how is customer data used while in the alexa cloud. the device-specific details in this paper are aimed primarily at the three amazon echo devices that can be managed with alexa for business-echo plus, echo (2 nd generation), and echo dot (2 nd generation). because echo show and echo spot can be used in conjunction with alexa for business, information specific to these two devices is also provided. information is presented in three sections. first is an end-to-end overview of the alexa system. next is a description of how echo devices detect their wake word and begin streaming audio to the cloud. last is a description of data retention and use within the alexa cloud. what is the alexa system? we must first understand what the alexa system is, and how it processes requests. for purposes of this discussion, the alexa system is comprised of echo devices listed above-the hardware and software that customers directly interact with and the cloud components-which have the majority of the 'smarts': automatic speech recognition, natural language understanding, and response. some responses are provided by third party services through 'skills.' the 3 rd-parties that write and publish those skills are responsible for their skill's behavior. to start, we begin with a very simple tour through the entire system, demonstrated with the example request of 'alexa, what is the weather,' so we can see how the request is picked up by an echo, sent through voice recognition, interpreted, acted upon, and then responded to figure: overview of echo and the alexa system"

Edwards, H. S.. (2017). Alexa Takes the Stand: Listening Devices Raise Privacy Issues.. Time

Show/hide publication abstract

"The article discusses the negative effect of the use of amazon echo, a smart speaker developed by [amazon.com](https://www.amazon.com), in the u.s., which became more dangerous as it has taken the consumer's privacy for information. it mentions the statement from joel reidenberg, a founding director of fordham university's center on law and information policy, regarding the matter. and also noted the u.s. privacy law."

Schönherr, L., Golla, M., Eisenhofer, T., Wiele, J., Kolossa, D., & Holz, T.. (2022). Exploring accidental triggers of smart speakers. Computer Speech and Language

Plain numerical DOI: 10.1016/j.csl.2021.101328

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Voice assistants like amazon's alexa, google's assistant, tencent's xiaowei, or apple's siri, have become the primary (voice) interface in smart speakers that can be found in millions of households. for privacy reasons, these speakers analyze every sound in their environment for their respective wake word like 'alexa,' 'jǐ?si?èr líng,' or 'hey siri,' before uploading the audio stream to the cloud for further processing. previous work reported on examples of an inaccurate wake word detection, which can be tricked using similar words or sounds like 'cocaine noodles' instead of 'ok google.' in this paper, we perform a comprehensive analysis of such accidental triggers, i.e., sounds that should not have triggered the voice assistant, but did. more specifically, we automate the process of finding accidental triggers and measure their prevalence across 11 smart speakers from 8 different manufacturers using everyday media such as tv shows, news, and other kinds of audio datasets. to systematically detect accidental triggers, we describe a method to artificially craft such triggers using a pronouncing dictionary and a weighted, phone-based levenshtein distance. in total, we have found hundreds of

accidental triggers. moreover, we explore potential gender and language biases and analyze the reproducibility. finally, we discuss the resulting privacy implications of accidental triggers and explore countermeasures to reduce and limit their impact on users' privacy. to foster additional research on these sounds that mislead machine learning models, we publish a dataset of more than 350 verified triggers as a research artifact."

Cho, E., Motalebi, N., Sundar, S. S., & Abdullah, S.. (2022). Alexa as an Active Listener: How Backchanneling Can Elicit Self-Disclosure and Promote User Experience. *Proceedings of the ACM on Human-Computer Interaction*

Plain numerical DOI: 10.1145/3555164

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Active listening is a well-known skill applied in human communication to build intimacy and elicit self-disclosure to support a wide variety of cooperative tasks. when applied to conversational uis, active listening from machines can also elicit greater self-disclosure by signaling to the users that they are being heard, which can have positive outcomes. however, it takes considerable engineering effort and training to embed active listening skills in machines at scale, given the need to personalize active-listening cues to individual users and their specific utterances. a more generic solution is needed given the increasing use of conversational agents, especially by the growing number of socially isolated individuals. with this in mind, we developed an amazon alexa skill that provides privacy-preserving and pseudo-random backchanneling to indicate active listening. user study (n = 40) data show that backchanneling improves perceived degree of active listening by smart speakers. it also results in more emotional disclosure, with participants using more positive words. perception of smart speakers as active listeners is positively associated with perceived emotional support. interview data corroborate the feasibility of using smart speakers to provide emotional support. these findings have important implications for smart speaker interaction design in several domains of cooperative work and social computing."

Lentzsch, C., Shah, S. J., Andow, B., Degeling, M., Das, A., & Enck, W.. (2021). Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem

Plain numerical DOI: 10.14722/ndss.2021.23111

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Amazon's voice-based assistant, alexa, enables users to directly interact with various web services through natural language dialogues. it provides developers with the option to create third-party applications (known as skills) to run on top of alexa. while such applications ease users' interaction with smart devices and bolster a number of additional services, they also raise security and privacy concerns due to the personal setting they operate in. this paper aims to perform a systematic analysis of the alexa skill ecosystem. we perform the first large-scale analysis of alexa skills, obtained from seven different skill stores totaling to 90,194 unique skills. our analysis reveals several limitations that exist in the current skill vetting process. we show that not only can a malicious user publish a skill

under any arbitrary developer/company name, but she can also make backend code changes after approval to coax users into revealing unwanted information. we, next, formalize the different skill-squatting techniques and evaluate the efficacy of such techniques. we find that while certain approaches are more favorable than others, there is no substantial abuse of skill squatting in the real world. lastly, we study the prevalence of privacy policies across different categories of skill, and more importantly the policy content of skills that use the alexa permission model to access sensitive user data. we find that around 23.3% of such skills do not fully disclose the data types associated with the permissions requested. we conclude by providing some suggestions for strengthening the overall ecosystem, and thereby enhance transparency for end-users."

Lau, J., Zimmerman, B., & Schaub, F.. (2018). "Alexa, Stop Recording": Mismatches between Smart Speaker Privacy Controls and User Needs. 14th Symposium on Usable Privacy and Security (SOUPS 2018)

Show/hide publication abstract

"Smart speakers, like amazon echo and google home, provide benefits and convenience through their integrated voice assistants, but also raise privacy concerns due to their continuously listening microphones. we studied users' privacy-seeking behaviors around these devices and their use of current privacy controls. through a diary study and in-home interviews with seventeen smart speaker users, we found users rarely engaged in privacy-seeking behaviors or utilized current privacy controls, which are currently not addressing their needs. our findings can inform the design of privacy controls in future smart speakers."

Hyma, J., Rama Krishna Murty, M., & Naveen, A.. (2021). Personalized privacy assistant for digital voice assistants: Case study on Amazon Alexa. International Journal of Knowledge-Based and Intelligent Engineering Systems

Plain numerical DOI: 10.3233/KES-210071

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"The advancements in modern technologies permit the invention of various digital devices which are controlled and activated by people's gestures, touch and even by one's voice. google assistant, iphone siri, amazon alexa etc., are most popular voice enabled devices which have grabbed the attention of digital gadget users. their usage definitely makes the life easier and comfortable. the other side of these smart enabled devices is incredible violation of the privacy. this happens due to their continuous listening to the user and data transmission over a public network to the third-party services. the work proposed in this paper attempts to overcome the existing privacy violation problem with the voice enabled devices. the main idea is to incorporate an intelligent privacy assistant that works based on the user preferences over their data."

Kim, J., Erdem, M., & Kim, B.. (2023). Hi Alexa, do hotel guests have privacy concerns with you?: A cross-cultural study. Journal of Hospitality Marketing and Management

Plain numerical DOI: 10.1080/19368623.2023.2251157

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"The purpose of this study is to examine the relationships among customer trust toward voice artificial intelligence (ai) in guestrooms, information privacy concerns associated with this technology, intention to use, and intention to stay at a hotel providing this technology. this study further examined whether the research model can be applied to different cultures by collecting data from u.s. and singaporean customers. the hypotheses were tested via structural equation modeling and multiple-group analysis. the findings indicated that trust toward voice ai had a positive effect on intention to use this technology in both groups, and this effect was stronger for the u.s. group. concern of information collection via voice ai had a negative effect on intention to use in both groups, and this effect was stronger for the singaporean group. intention to use voice ai in guestrooms was positively related to intention to stay at a hotel providing this technology."

Ford, M., & Palmer, W.. (2019). Alexa, are you listening to me? An analysis of Alexa voice service network traffic. *Personal and Ubiquitous Computing*

Plain numerical DOI: 10.1007/s00779-018-1174-x

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"With approximately 8.2 million echo family devices sold since 2014, amazon controls 70% of the intelligent personal assistant market. amazon's alexa voice service (avs) provides voice control services for amazon's echo product line and various home automation devices such as thermostats and security cameras. in november 2017, amazon expanded alexa services into the business intelligent assistant market with alexa for business. as corporations integrate alexa into their corporate networks, it is important that information technology security stakeholders understand alexa's audio streaming network behavior in order to properly implement security countermeasures and policies. this paper contributes to the intelligent personal assistant knowledge domain by providing insight into amazon voice services behavior by analyzing the network traffic of two echo dots over a 21-day period. the echo dots were installed in a private residence, and at no time during the experiment did family members or house guests purposely interact with the echos. all recorded audio commands were inadvertent. using a k-mean cluster analysis, this study established a quantifiable avs network signature. then, by comparing that avs signature and logged alexa audio commands to the 21-day network traffic dataset, this study confirmed disabling the echo's microphone, with the on/off button, prohibits audio recording and streaming to alexa voice service. with 30–38% of echo dots' spurious audio recordings were human conversations, these findings support the echo dot recorded private home conversations and not all audio recordings are properly logged the alexa application. while further alexa network traffic studies are needed, this study offers a network signature capable of identifying avs network traffic."

Uysal, E., Alavi, S., & Bezençon, V.. (2022). Trojan horse or useful helper? A relationship perspective on artificial intelligence assistants with humanlike features. *Journal of the Academy of Marketing Science*

Plain numerical DOI: 10.1007/s11747-022-00856-9

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Artificial intelligence assistants (aias) such as alexa are prevalent in consumers’ homes. owing to their powerful artificial intelligence, consumers may perceive that aias have a mind of their own, that is, they anthropomorphize them. past marketing research points to beneficial effects of aia anthropomorphism for consumers and companies, while potential harmful effects have not been empirically explored. in examining both beneficial and harmful effects, this paper adopts a relationship perspective. indeed, consumers spend large amounts of time with their aias, potentially developing a relationship over time that builds on an exchange of benefits and (psychological) costs. a preliminary survey and user interviews, a field study and a field experiment with aia users show that aia anthropomorphism may threaten users’ identity, which disempowers them, creates data privacy concerns and ultimately undermines their well-being. these harmful effects particularly emerge in close, long relationships. the field experiment uncovers three empowering interventions which attenuate harmful effects of aia anthropomorphism in relationships with consumers. with ai-powered technologies taking larger roles in our daily lives, our research highlights key future directions to investigate the permanent ongoing nature of the consumer–ai relationships.”

Lit, Y., Kim, S., & Sy, E.. (2021). A survey on amazon alexa attack surfaces. In 2021 IEEE 18th Annual Consumer Communications and Networking Conference, CCNC 2021

Plain numerical DOI: 10.1109/CCNC49032.2021.9369553

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Since being launched in 2014, alexa, amazon’s versatile cloud-based voice service, is now active in over 100 million households worldwide [1]. alexa’s user-friendly, personalized vocal experience offers customers a more natural way of interacting with cutting-edge technology by allowing the ability to directly dictate commands to the assistant. now in the present year, the alexa service is more accessible than ever, available on hundreds of millions of devices from not only amazon but third-party device manufacturers. unfortunately, that success has also been the source of concern and controversy. the success of alexa is based on its effortless usability, but in turn, that has led to a lack of sufficient security. this paper surveys various attacks against amazon alexa ecosystem including attacks against the frontend voice capturing and the cloud backend voice command recognition and processing. overall, we have identified six attack surfaces covering the lifecycle of alexa voice interaction that spans several stages including voice data collection, transmission, processing and storage. we also discuss the potential mitigation solutions for each attack surface to better improve alexa or other voice assistants in terms of security and privacy.”

Neville, S. J.. (2020). Eavesmining: A critical audit of the amazon echo and alexa conditions of use. Surveillance and Society

Plain numerical DOI: 10.24908/ss.v18i3.13426

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“The emergence of smart speakers and voice-activated personal assistants (vapas) calls for updated scrutiny and theorization of auditory surveillance. this paper introduces the neologism and concept of ‘eavesmining’ (eavesdropping + data mining) to characterize a mode of surveillance that operates on the edge of acoustic space and digital infrastructure. in contributing to a sonic epistemology of surveillance, i explain how eavesmining platforms and processes burrow the voice as a medium between sound and data and articulate the acoustic excavation of smart environments. the paper discusses eavesmining in relation to theories of dataveillance, the sensor society, and surveillance capitalism before outlining the potential contributions offered by a theoretical alignment with sound studies literature. the paper centers on an empirical case study of the amazon echo and alexa conditions of use. by conducting a discourse analysis of amazon’s end user agreements (euas), i provide evidence in support of growing privacy and surveillance concerns produced by amazon’s eavesmining platform that are obfuscated by the illegibility of the documents.”

Edu, J. S., Such, J. M., & Suarez-Tangil, G.. (2021). Smart Home Personal Assistants: A Security and Privacy Review. ACM Computing Surveys

Plain numerical DOI: 10.1145/3412383

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Smart home personal assistants (spa) are an emerging innovation that is changing the means by which home users interact with technology. however, several elements expose these systems to various risks: (i) the open nature of the voice channel they use, (ii) the complexity of their architecture, (iii) the ai features they rely on, and (iv) their use of a wide range of underlying technologies. this article presents an in-depth review of spa’s security and privacy issues, categorizing the most important attack vectors and their countermeasures. based on this, we discuss open research challenges that can help steer the community to tackle and address current security and privacy issues in spa. one of our key findings is that even though the attack surface of spa is conspicuously broad and there has been a significant amount of recent research efforts in this area, research has so far focused on a small part of the attack surface, particularly on issues related to the interaction between the user and the spa devices. to the best of our knowledge, this is the first article to conduct such a comprehensive review and characterization of the security and privacy issues and countermeasures of spa.”

Gieselmann, M., & Sassenberg, K.. (2022). The More Competent, the Better? The Effects of Perceived Competencies on Disclosure Towards Conversational Artificial Intelligence. Social Science Computer Review

Plain numerical DOI: 10.1177/08944393221142787

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Conversational ai (e.g., google assistant or amazon alexa) is present in many people’s everyday life and, at the same time, becomes more and more capable of solving more complex tasks. however, it is unclear how the growing capabilities of conversational ai affect people’s disclosure towards the system as previous research has revealed mixed effects of technology competence. to address this research question, we propose a framework systematically disentangling conversational ai competencies along the lines of the dimensions of human competencies suggested by the action regulation theory. across two correlational studies and three experiments (ntotal = 1453), we investigated how these competencies differentially affect users’ and non-users’ disclosure towards conversational ai. results indicate that intellectual competencies (e.g., planning actions and anticipating problems) in a conversational ai heighten users’ willingness to disclose and reduce their privacy concerns. in contrast, meta-cognitive heuristics (e.g., deriving universal strategies based on previous interactions) raise privacy concerns for users and, even more so, for non-users but reduce willingness to disclose only for non-users. thus, the present research suggests that not all competencies of a conversational ai are seen as merely positive, and the proposed differentiation of competencies is informative to explain effects on disclosure.”

Mou, Y., & Meng, X.. (2023). Alexa, it is creeping over me – Exploring the impact of privacy concerns on consumer resistance to intelligent voice assistants. *Asia Pacific Journal of Marketing and Logistics*

Plain numerical DOI: 10.1108/APJML-10-2022-0869

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Purpose: with the upgrade of natural language interaction technology, the simulation extension of intelligent voice assistants (ivas) and the uncertainty of products and services have received more and more attention. however, most of the existing research focuses on investigating the application of theories to explain consumer behavior related to intention to use and adopt ivas, while ignoring the impact of its privacy issues on consumer resistance. this article especially examines the negative impact of artificial intelligence-based ivas’ privacy concerns on consumer resistance, and studies the mediating effect of perceived creepiness in the context of privacy cynicism and privacy paradox and the moderating effect of anthropomorphized roles of ivas and perceived corporate social responsibility (csr) of ivas’ companies. the demographic variables are also included. design/methodology/approach: based on the theory of human–computer interaction (hci), this study addresses the consumer privacy concerns of ivas, builds a model of the influence mechanism on consumer resistance, and then verifies the mediating effect of perceived creepiness and the moderating effect of anthropomorphized roles of ivas and perceived csr of ivas companies. this research explores underlying mechanism with three experiments. findings: it turns out that consumers’ privacy concerns are related to their resistance to ivas through perceived creepiness. the servant (vs. partner) anthropomorphized role of ivas is likely to induce more privacy concerns and in turn higher resistance. at the same time, when the company’s csr is perceived high, the impact of the concerns of ivas’ privacy issues on consumer resistance will be weakened, and the intermediary mechanism of perceiving creepiness in hci and anthropomorphism of

new technology are further explained and verified. the differences between different age and gender are also revealed in the study. originality/value: the research conclusions have strategic reference significance for enterprises to build the design framework of ivas and formulate the response strategy of ivas' privacy concerns. and it offers implications for researchers and closes the research gap of ivas from the perspective of innovation resistance."

Developing a Measure of Social, Ethical, and Legal Content for Intelligent Cognitive Assistants. (2021). Journal of Strategic Innovation and Sustainability

Plain numerical DOI: 10.33423/jsis.v16i3.4438

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"We address the issue of consumer privacy against the backdrop of the national priority of maintaining global leadership in artificial intelligence, the ongoing research in artificial cognitive assistants, and the explosive growth in the development and application of voice activated personal assistants (vapas) such as alexa and siri, spurred on by the needs and opportunities arising out of the covid-19 global pandemic. we first review the growth and associated legal issues of the of vapas in private homes, banks, healthcare, and education. we then summarize the policy guidelines for the development of vapas. then, we classify these into five major categories with associated traits. we follow by developing a relative importance weight for each of the traits and categories; and suggest the establishment of a rating system related to the legal, ethical, functional, and social content policy guidelines established by these organizations. we suggest the establishment of an agency that will use the proposed rating system to inform customers of the implications of adopting a particular vapa in their sphere."

Liu, Y., Xiang, Z., Seong, E. J., Kapadia, A., & Williamson, D. S.. (2021). Defending Against Microphone-Based Attacks with Personalized Noise. Proceedings on Privacy Enhancing Technologies

Plain numerical DOI: 10.2478/popets-2021-0021

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Voice-activated commands have become a key feature of popular devices such as smartphones, home assistants, and wearables. for convenience, many people configure their devices to be 'always on' and listening for voice commands from the user using a trigger phrase such as 'hey siri,' 'okay google,' or 'alexa.' however, false positives for these triggers often result in privacy violations with conversations being inadvertently uploaded to the cloud. in addition, malware that can record one's conversations remains a significant threat to privacy. unlike with cameras, which people can physically obscure and be assured of their privacy, people do not have a way of knowing whether their microphone is indeed off and are left with no tangible defenses against voice based attacks. we envision a general-purpose physical defense that uses a speaker to inject specialized obfuscating 'babble noise' into the microphones of devices to protect against automated and human based attacks. we present a comprehensive study of how specially crafted, personalized 'babble' noise ('mybabble') can be effective at moderate signal-to-noise ratios and can provide a viable defense against

microphone based eavesdropping attacks.”

Javed, Y., Sethi, S., & Jadoun, A.. (2019). Alexa’s voice recording behavior: A survey of user understanding and awareness. In ACM International Conference Proceeding Series

Plain numerical DOI: 10.1145/3339252.3340330

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“The use of amazon’s virtual assistant alexa in controlling smart home devices is on the rise. the convenience provided by an alexa-enabled device comes at the cost of alexa service’s voice recording and storage behavior, raising privacy concerns. amazon claims to record and store voice data in the cloud only when the wake word is spoken. however, alexa records user’s voice even at times when the wake word is not used. though short, these recordings can potentially contain a sensitive conversation between individuals. anyone in the possession of the amazon alexa mobile application with which the smart device is registered, can access these recordings. this paper aims to investigate alexa users’ understanding and awareness of its voice recording and storage behavior. we conducted an amazon turk study on 113 amazon echo owners. our results show that 91% of the participants had at-least one instance of unintended voice recording. 53.09% of our participants reported that a subset of these unlabeled recordings did not contain any voice commands. although a majority of the participants (64.6%) were aware that alexa stores data in amazon cloud, the participants lacked awareness of 1) intended and unintended voice data being recorded and stored, 2) entities who can potentially access these voice recordings, and 3) voice recording deletion. having technical/cs background did not influence the participants responses. however, the participants who were strongly concerned about privacy (fundamentalists) seemed to have a better understanding of alexa’s voice recording storage behavior.”

Munn, L.. (2019). “ALEXA, CAN I TRUST YOU?”: SMALL SISTERS AND FRIENDLY POWER.

AoIR Selected Papers of Internet Research

Plain numerical DOI: 10.5210/spir.v2019i0.11012

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“How is trust fabricated today? this paper argues that the persona of ‘alexa’ bypasses concerns around surveillance and privacy, defusing anxieties not via the rationality of a convincing argument but through the relationality of alexa as a singular presence. in many respects alexa is actually more invasive than other technologies. amazon has encroached into the very heart of the home. moreover, the company’s patents delve further into the subject through voice identification, mood monitoring, and health detection. but this encroachment is carried out by her, rather than it, a warm and welcoming persona. the team’s aim is to develop something that is friendly, can turn off your lights, chat about anything, and empathize when you’re having a bad day (mcgirt 2018). the goal is to construct something chattier, more affective and emotionally attuned. in doing so, alexa embodies what theorist byung-chul han (2017) has called ‘friendly power.’ the result is that alexa feels different. instead of an algorithmic bundle of technologies, alexa is experienced as an affective persona. alexa thus delves deeper into the

inner life of the subject while shrugging off the anxieties associated with cold, command-and-control technologies. rather than an all-seeing eye, she is an always listening voice, a friendly companion. and rather than emanating from a central agency, she is co-located with the user. if big brother no longer characterizes contemporary power (harcourt 2015), alexa might be described as a 'small sister.' small sisters work alongside instead of above. small sisters are multiple, sited, and supple."

Martínez, D., Calle, E., Jové, A., & Pérez-Solà, C.. (2022). Web-tracking compliance: websites' level of confidence in the use of information-gathering technologies: Web-tracking level of confidence. Computers and Security

Plain numerical DOI: 10.1016/j.cose.2022.102873

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"With the emergence of new technologies and the generalized use of social media, corporations have an invested economic interest in employing web-tracking techniques, but there is also the issue of protecting users' privacy. in this field of research, only few articles introduce methods to evaluate website compliance in the use of current web-tracking techniques. moreover, evaluating the level of compliance requires, in the majority of cases, manually implementing an extensive data analysis. in this paper, we present four new algorithms (cia, cda, bda, and sca) and a novel measure (wloc) to evaluate user tracking compliance in websites and the level of confidence in the use of information-gathering technologies, by employing the recently published website evidence collector (wec) software from the european data protection supervisor (edps). the paper also showcases a case study of the top 500 websites most visited by alexa in spain to evaluate the performance of the presented algorithms and metrics. results reveal a novel procedure for obtaining categorized websites' compliance and confidence levels of a set of websites under the current european legislation, thus updating and enhancing some of the previous research work."

Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., & Lee, A. J.. (2022). Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. Proceedings of the ACM on Human-Computer Interaction

Plain numerical DOI: 10.1145/3555089

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Smart voice assistants such as amazon alexa and google home are becoming increasingly pervasive in our everyday environments. despite their benefits, their miniaturized and embedded cameras and microphones raise important privacy concerns related to surveillance and eavesdropping. recent work on the privacy concerns of people in the vicinity of these devices has highlighted the need for 'tangible privacy', where control and feedback mechanisms can provide a more assured sense of whether the camera or microphone is 'on' or 'off'. however, current designs of these devices lack adequate mechanisms to provide such assurances. to address this gap in the design of smart voice assistants, especially in the case of disabling microphones, we evaluate several designs that incorporate (or not) tangible control and feedback mechanisms. by comparing people's perceptions of risk, trust, reliability,

usability, and control for these designs in a between-subjects online experiment (n=261), we find that devices with tangible built-in physical controls are perceived as more trustworthy and usable than those with non-tangible mechanisms. our findings present an approach for tangible, assured privacy especially in the context of embedded microphones."

Oliveira, G. G. de, Lizarelli, F. L., Teixeira, J. G., & Mendes, G. H. de S.. (2023). Curb your enthusiasm: Examining the customer experience with Alexa and its marketing outcomes. *Journal of Retailing and Consumer Services*

Plain numerical DOI: 10.1016/j.jretconser.2022.103220

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Interactive voice assistants (ivas) are intelligent conversational agents capable of communicating with users using natural language. although ivas are more frequent in our lives, customer experience research with these agents is still in its infancy. this article aims to identify the factors that form the customer experience (cx) with alexa and assesses its impact on traditional marketing outcomes: satisfaction and recommendation. this research presents a conceptual model of cx with ivas and an empirical validation of the model using structural equation modelling based on a sample of 580 iva users. the results confirm that cx is a multidimensional higher-order construct composed of six factors (usefulness, ease of use, trust, privacy concerns, communication skills, and enjoyment). we also highlight the positive impact of experience on satisfaction and recommendation. finally, we test the enthusiasm moderating role, showing its negative influence on the investigated relationships. theoretical and practical implications are discussed."

Pal, D., Babakerkhell, M. D., & Zhang, X.. (2021). Exploring the Determinants of Users' Continuance Usage Intention of Smart Voice Assistants. *IEEE Access*

Plain numerical DOI: 10.1109/ACCESS.2021.3132399

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"The use of personal voice-assistants like amazon alexa and google assistant has been on the rise recently. to ensure a long-term success and widespread diffusion of these products it is important to evaluate their continued usage scenario instead of the initial adoption intention. majority of research evaluating the continuance usage scenario do so via an expectation-confirmation approach. however, in this work a user engagement-based approach is taken for evaluating the utilitarian and hedonic attitudes of the users towards the continued usage scenario. this is augmented with additional contextual constructs like trust, privacy risk, and satisfaction. at present, there is little empirical evidence of user engagement with voice-assistants. moreover, the present work focuses on the continuance usage of late adopters by considering two unique personal factors (slowness of adoption and skepticism). by evaluating the engagement aspect of the laggard group, the current findings contribute to theory by providing a better understanding of how the proposed antecedents determine the continuance intention. data is collected from 244 late adopters of voice-assistants who use these devices in their daily life for building the research framework. all the proposed hypotheses are

supported except the effect of privacy risk. the implications for both theory and practice are provided based on the findings."

Burkett, C. B.. (2018). "I Call Alexa to the Stand": The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology. *Vanderbilt Journal of Entertainment & Technology Law*

Show/hide publication abstract

"This note offers a solution to the unique privacy issues posed by the increasingly humanlike interactions users have with virtual assistants, such as amazon's alexa, which accompany smart-home technology. these interactions almost certainly result in the users engaging in the cognitive phenomenon of anthropomorphism-more specifically, an assignment of agency. this is a phenomenon that has heretofore been ignored in the legal context, but both the rapidity of technological advancement and inadequacy of current applicable legal doctrine necessitate its consideration now. since users view these anthropomorphized virtual assistants as persons rather than machines, the law should treat them as such. to accommodate this reality, either the courts or congress should grant them legal personhood. this can be accomplished through the application of an objective test that is satisfied by the establishment of social and moral connections with these virtual assistants. further, due to the paramount privacy concerns resulting from this technology's use within the home, courts should establish a new privilege that protects the communications between users and their virtual assistants." Gupta, A., & Mishra, M.. (2022). Ethical Concerns While Using Artificial Intelligence in Recruitment of Employees. *Business Ethics and Leadership*

Plain numerical DOI: 10.21272/bel.6(2).6-11.2022

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Artificial intelligence has evolved as an alternative to human intelligence. it affects the lives of billions of people. it mimics humans by solving problems and understanding the task. these artificial intelligence technologies must have some moral values and ethics incorporated within itself. the usage of ai is growing worldwide, posing more ethical issues to consider. in recent years, many companies have used various artificial intelligence tools such as chatbots and face recognition software for fulfilling their hiring needs. this research work will focus on such devices that help manage one of the important functions of human resources: recruitment. it will identify various challenges and ethical issues that a firm faces while assimilating artificial intelligence tools in the process of recruitment. the hiring companies need to make the job seekers realize that ai-powered tools would be free from discrimination and safeguard privacy. the purpose of the study is to identify the ethical issues while incorporating artificial intelligence into hiring needs. the study will be based on reviews and features of applications. the study mentions various applications whose features might be unethical for job seekers. findings reveal that the significant unethical issues faced by the hiring companies are data privacy and unconscious biasness. the biasness is due to the algorithm that works according to the inputs fed to build it, and the programmer might have subconscious biasness in his mind. ai has restored concerns regarding privacy and data protection. according to a report by unesco, women make up only 22% of all ai professionals. gender prejudices and stereotyping are perpetuated in ai technologies due to their underrepresentation in the sector. virtual personal assistants like siri, alexa,

and cortana are 'female' by default, which is no accident. the submissiveness they display is an illustration of how artificial intelligence (ai) might continue to support and extend gender bias in our society."

Natale, S., & Cooke, H.. (2021). Browsing with Alexa: Interrogating the impact of voice assistants as web interfaces. *Media, Culture and Society*

Plain numerical DOI: 10.1177/0163443720983295

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Voice assistants such as siri, alexa, and google assistant have recently been the subject of lively debates in regard to issues such as artificial intelligence, surveillance, gender stereotypes, and privacy. less attention, however, has been given to the fact that voice assistants are also web interfaces that might impact on how the web is accessed, understood and employed by users. this article aims to advance work in this context by identifying a range of issues that should spark additional reflections and discussions within communication and media studies and related fields. in particular, the article focuses on three key issues that have to do with long-standing discussions about the social and political impact of the internet: the role of web platforms in shaping information access, the relationship between production and consumption online, and the role of affect in informing engagement with web resources. considering these issues in regard to voice assistants not only helps contextualize these technologies within existing debates in communication and media studies, but also highlights that voice assistants pose novel questions to internet research, challenging assumptions of what the web looks like as speech becomes one of the key ways to access resources and information online."

Oulousian, E., Chung, S. H., Ganni, E., Razaghizad, A., Zhang, G., Avram, R., & Sharma, A.. (2023). Voice-Based Screening for SARS-CoV-2 Exposure in Cardiovascular Clinics (VOICE-COVID-19-II): Protocol for a Randomized Controlled Trial. *JMIR Research Protocols*

Plain numerical DOI: 10.2196/41209

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"Background: the covid-19 pandemic has disrupted the health care system, limiting health care resources such as the availability of health care professionals, patient monitoring, contact tracing, and continuous surveillance. as a result of this significant burden, digital tools have become an important asset in increasing the efficiency of patient care delivery. digital tools can help support health care institutions by tracking transmission of the virus, aiding in the screening process, and providing telemedicine support. however, digital health tools face challenges associated with barriers to accessibility, efficiency, and privacy-related ethical issues. objective: this paper describes the study design of an open-label, noninterventional, crossover, randomized controlled trial aimed at assessing whether interactive voice response systems can screen for sars-cov-2 in patients as accurately as standard screening done by people. the study aims to assess the concordance and interrater reliability of symptom screening done by amazon alexa compared to manual screening done by research coordinators. the perceived level of comfort of patients when interacting with voice response systems

and their personal experience will also be evaluated. methods: a total of 52 patients visiting the heart failure clinic at the royal victoria hospital of the mcgill university health center, in montreal, quebec, will be recruited. patients will be randomly assigned to first be screened for symptoms of sars-cov-2 either digitally, by amazon alexa, or manually, by the research coordinator. participants will subsequently be crossed over and screened either digitally or manually. the clinical setup includes an amazon echo show, a tablet, and an uninterrupted power supply mounted on a mobile cart. the primary end point will be the interrater reliability on the accuracy of randomized screening data performed by amazon alexa versus research coordinators. the secondary end point will be the perceived level of comfort and app engagement of patients as assessed using 5-point likert scales and binary mode responses. results: data collection started in may 2021 and is expected to be completed in fall 2022. data analysis is expected to be completed in early 2023. conclusions: the use of voice-based assistants could improve the provision of health services and reduce the burden on health care personnel. demonstrating a high interrater reliability between amazon alexa and health care coordin...

Sabir, A., Lafontaine, E., & Das, A.. (2022). Hey Alexa, Who Am I Talking to?: Analyzing Users' Perception and Awareness Regarding Third-party Alexa Skills. In Conference on Human Factors in Computing Systems – Proceedings

Plain numerical DOI: 10.1145/3491102.3517510

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“The amazon alexa voice assistant provides convenience through automation and control of smart home appliances using voice commands. amazon allows third-party applications known as skills to run on top of alexa to further extend alexa’s capability. however, as multiple skills can share the same invocation phrase and request access to sensitive user data, growing security and privacy concerns surround third-party skills. in this paper, we study the availability and effectiveness of existing security indicators or a lack thereof to help users properly comprehend the risk of interacting with different types of skills. we conduct an interactive user study (inviting active users of amazon alexa) where participants listen to and interact with real-world skills using the official alexa app. we find that most participants fail to identify the skill developer correctly (i.e., they assume amazon also develops the third-party skills) and cannot correctly determine which skills will be automatically activated through the voice interface. we also propose and evaluate a few voice-based skill type indicators, showcasing how users would benefit from such voice-based indicators.”

Chubb, J., Missaoui, S., Concannon, S., Maloney, L., & Walker, J. A.. (2022). Interactive storytelling for children: A case-study of design and development considerations for ethical conversational AI. International Journal of Child-Computer Interaction

Plain numerical DOI: 10.1016/j.ijcci.2021.100403

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

“Conversational artificial intelligence (cai) systems and intelligent personal assistants (ipa), such as alexa, cortana, google home and siri are becoming ubiquitous in our lives, including those of children,

the implications of which is receiving increased attention, specifically with respect to the effects of these systems on children's cognitive, social and linguistic development. recent advances address the implications of cai with respect to privacy, safety, security, and access. however, there is a need to connect and embed the ethical and technical aspects in the design. using a case-study of a research and development project focused on the use of cai in storytelling for children, this paper reflects on the social context within a specific case of technology development, as substantiated and supported by argumentation from within the literature. it describes the decision making process behind the recommendations made on this case for their adoption in the creative industries. further research that engages with developers and stakeholders in the ethics of storytelling through cai is highlighted as a matter of urgency."

Jang, D., Jhala, R., Lerner, S., & Shacham, H.. (2010). An empirical study of privacy-violating information flows in JavaScript web applications. In Proceedings of the ACM Conference on Computer and Communications Security

Plain numerical DOI: 10.1145/1866307.1866339

[DOI URL](#)

[directSciHub download](#)

Show/hide publication abstract

"The dynamic nature of javascript web applications has given rise to the possibility of privacy violating information flows. we present an empirical study of the prevalence of such flows on a large number of popular websites. we have (1) designed an expressive, fine-grained information flow policy language that allows us to specify and detect different kinds of privacy-violating flows in javascript code, (2) implemented a new rewriting-based javascript information flow engine within the chrome browser, and (3) used the enhanced browser to conduct a large-scale empirical study over the alexa global top 50,000 websites of four privacyviolating flows: cookie stealing, location hijacking, history sniffing, and behavior tracking. our survey shows that several popular sites, including alexa global top-100 sites, use privacy-violating flows to exfiltrate information about users' browsing behavior. our findings show that steps must be taken to mitigate the privacy threat from covert flows in browsers. copyright 2010 acm."

ZENOR, J.. (2021). If you see something, say something: Can artificial intelligence have a duty to report dangerous behavior in the home?. Denver Law Review

Show/hide publication abstract

"Artificial intelligence (ai) digital assistants, such as amazon's echo alexa and apple's siri, are becoming quite common in our homes. today, these voices typically come from a small speaker. but soon, they will be replaced by devices that appear more human than robot. as a result, our relationships with them will change. we will talk to them and share information, including our secrets, with them. of course, we will have to trust them with this information. but should we? if an ai is in the home and monitoring a person, what should it do if someone is exhibiting signs of alcoholism, depression, or violence? accordingly, this article postulates how changes in our personal relationship with ai could lead to changes in how privacy protections are viewed. first, this article examines nascent issues of ai assistants publicizing private activities and how these issues could evolve in the future. next, this article outlines privacy law as it pertains to activity in the home. finally, this article postulates how cultural expectations of privacy could erode in the future and offers suggestions on how to model

laws that balance privacy with public safety."

Category

1. General

Date Created

25. December 2023

Author

web45