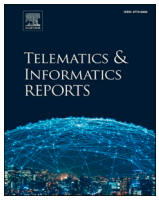
Telematics and Informatics Reports 11 (2023) 100092

Contents lists available at ScienceDirect

Telematics and Informatics Reports

journal homepage: www.elsevier.com/locate/teler



# The intersection of targeted advertising and security: Unraveling the mystery of overheard conversations

Mohamed Aly Bouke [a,*], Azizol Abdullah [1,a], Sameer Hamoud ALshatebi [1,a], Saleh Ali Zaid [1,a], Hayate El Atigh [1,b]

[a] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang 43400, Malaysia
[b] Departement Computer Engineering, Faculty of Computer Engineering, Bandirma Onyedi Eylul University, Balikesir 10200, Turkey

ARTICLE INFO

*Keywords:*
Targeted advertising
Voice recognition technology
User privacy
Security implications
Overheard conversations

ABSTRACT

This paper explores targeted advertising, focusing on voice recognition technology and its potential effects on user privacy, assessing the advantages and challenges of such advertising methods. By emphasizing the need to balance marketing efficacy and user privacy protection, the analysis delves into the evolution, current state, and potential applications of voice recognition technology in targeted advertising while considering ethical and legal aspects. Security implications of overheard conversations are also addressed, highlighting the importance of user consent, awareness, and legal frameworks. Strategies for preserving user privacy are proposed, encompassing privacy-enhancing technologies, policy recommendations, consumer awareness, and education efforts. This paper contributes to the ongoing discourse on balancing advertising efficiency and user privacy in today's digital landscape. It provides a comprehensive analysis and valuable insights for stakeholders, including advertisers, policymakers, and users.

## 1. Introduction

Digital advertising has undergone a rapid transformation in recent years, driven by advancements in technology and the increasing ubiquity of internet access. As a result, marketers have developed sophisticated methods for reaching their target audiences with relevant content. Among these, targeted advertising has emerged as a dominant strategy for connecting with consumers more personally, accounting for a significant portion of digital advertising spending [1]. Moreover, targeted advertising is a marketing approach that leverages data and technology to deliver tailored messages to specific user segments [2]. This method collects and analyses user data, including browsing history, search queries, demographic information, and social media activity. Advertisers use this wealth of data to create detailed profiles of individual users, which are then used to serve relevant ads that align with users' interests, needs, or preferences. The primary goal of targeted advertising is to increase the likelihood of user engagement and conversion, thus enhancing the effectiveness of marketing campaigns [3].

Voice recognition technology has experienced significant advancements in recent years, becoming integral to various digital products and services. This technology relies on complex algorithms and artificial intelligence to process and analyze human speech, allowing devices to understand spoken language and respond accordingly. Smartphones, smart speakers, and virtual assistants like Siri, Alexa, and Google Assistant are all devices that utilize voice recognition capabilities. As voice recognition has become more accurate and widespread, its potential applications have expanded, including the possibility of being used in targeted advertising [4].

Personal experiences and anecdotal evidence, such as users reporting targeted ads related to private conversations, suggest that some users may receive targeted advertisements related to topics they have discussed on calls, raising concerns about security and privacy [5]. While it is unclear if advertisers are utilizing voice recognition technology to listen to users' conversations, such a connection warrants investigation. This phenomenon raises questions about the extent to which voice data is accessed, the legal and ethical frameworks surrounding its use, and potential implications for user privacy and security.

The intersection of voice recognition technology and targeted

* Corresponding author.
*E-mail address:* bouke@ieee.org (M.A. Bouke).
[1] These authors contributed equally to this work.

https://doi.org/10.1016/j.teler.2023.100092
Received 26 April 2023; Received in revised form 10 August 2023; Accepted 12 August 2023
Available online 13 August 2023

advertising presents a complex and underexplored area of concern. With anecdotal evidence suggesting that private conversations may influence targeted advertisements, there is a pressing need to investigate the underlying mechanisms and ethical considerations. The ambiguity surrounding the utilization of voice data by advertisers, the legal frameworks governing its use, and the broader implications for user privacy and security necessitate a comprehensive and multifaceted investigation.

The novelty of this work lies in its interdisciplinary approach, bridging gaps between technology, law, ethics, and marketing. By providing a comprehensive analysis of how overheard conversations might be used in targeted advertising, this research extends beyond mere technological considerations to include legal and ethical dimensions. It offers a unique perspective synthesizing insights from various fields, contributing to academic discourse and practical applications in the industry. In addition, it represents a promising effort to explore a critical societal issue with a blend of empirical analysis and theoretical exploration, setting a precedent for future studies in this domain.

Moreover, the main contribution of this work is:

- Comprehensive Analysis: This research comprehensively analyses the mechanisms through which overheard conversations can be utilized for targeted advertising. It delves into the technological, ethical, and legal dimensions, offering a multifaceted perspective lacking in the existing literature.
- Integration of e-Privacy Regulations: By incorporating a detailed examination of e-Privacy regulations, this paper extends the discourse beyond mere technological considerations. It explores the legal landscape governing these practices, summarizing common e-Privacy laws and discussing their implications for users and businesses.
- Contribution to Theory and Practice: This research contributes to the theoretical understanding of targeted advertising and voice recognition technology and offers practical insights for stakeholders. It bridges the gap between theory and practice, providing actionable recommendations for advertisers, technology developers, policymakers, and users.
- Interdisciplinary Perspective: Drawing on literature from marketing, information technology, law, and ethics, this research adopts a multidisciplinary perspective. It synthesizes insights from various fields to provide a holistic understanding of the complex interplay between targeted advertising, voice recognition technology, and user privacy.

The remainder of this paper is organized into several key sections. Section 2: Literature Review reviews the relevant literature on targeted advertising, voice recognition technology, and the intersection between these two areas, focusing on user privacy and security implications. Section 3: Methodology details the research methodology, including the research paradigm that guides the study. Section 4: The Mechanism of Targeted Advertising explores the mechanisms behind targeted advertising, including a subsection on voice recognition and its role in advertising. Section 5: Security Implications of Overheard Conversations discusses the security implications of overheard conversations and includes strategies for protecting user privacy. Finally, Section 6: Conclusion concludes the paper, summarizing the findings and offering insights into the research implications.

## 2. Literature review

This section reviews relevant literature on targeted advertising, voice recognition technology, and the intersection between these two areas, focusing on user privacy and security implications. The discussion synthesizes the findings from various sources to provide a solid foundation for understanding the context of the paper.

A significant body of literature has examined the various aspects of targeted advertising, including its effectiveness, mechanism, and potential ethical concerns associated with data collection and privacy. Englehardt and Narayanan [6] extensively analyze online tracking techniques and data collection, focusing on the role of third-party data brokers and the commodification of user data. Lambrecht and Tucker [7] discuss using algorithms and data-driven approaches to create targeted advertisements, emphasizing the need to understand and mitigate potential biases in these algorithms.

Voice recognition technology has evolved rapidly in recent years, leading to various applications in various fields. Huang et al. [8] provide a historical perspective on speech recognition, tracing its development from early experimental systems to sophisticated algorithms and AI-driven approaches today. Elbaghazaoui et al. [4] present a literature review on voice recognition technology with user profiling. It aims to provide a comprehensive overview of human voice recognition in the significant data era, discussing techniques, use cases, and challenges.

Although limited literature explicitly examines the connection between overheard conversations and targeted advertising, several studies have explored related topics. For instance, Wu et al. [9] discuss the role of user behavior analysis in the context of misinformation on social media and its implications for targeted advertising. Although not directly addressing voice recognition technology, this study illustrates the potential for advanced data analysis techniques to influence online content users are exposed to.

Iqbal et al. [10] address privacy concerns in intelligent speakers by developing an auditing framework to measure data collection, usage, and sharing within the Amazon intelligent speaker ecosystem. The findings reveal that Amazon and third parties collect interaction data, which is used for targeted advertising on and off-platform. The study also highlights a lack of clear disclosure in privacy policies regarding these operational practices.

Jesus and Pandit [11] explore the concept of 'Consent Receipts' as a means to empower users in the context of online privacy and data protection. It conducts an extensive literature review to analyze Consent Receipts' requirements, uses, and benefits and identifies properties, needs, and new web-support mechanisms. The feasibility of Consent Receipts is demonstrated through proofs-of-concept in real-world use cases, including privacy policy acceptance, consent dialogues or cookie banners, and verbal interactions with Amazon Alexa.

Acosta and Reinhardt [12] examine end-user adoption of Voice-controlled Digital Assistants (VCDAs) and their associated privacy issues. To enhance privacy protection in VCDAs, the authors evaluate privacy concerns, assess existing GDPR solutions, and propose new research directions and mitigation strategies.

Moreover, as targeted advertising and voice recognition technologies become more pervasive, user privacy and security concerns have garnered increasing attention. Himeur et al. [13] provide a comprehensive overview of current research, taxonomy, and applications for analyzing security and privacy issues in contemporary recommender systems (RSs). The article critically evaluates existing frameworks and highlights emerging privacy and security research directions.

Atlam and Wills [14] discussed the issues posed by the Internet of Things (IoT) revolution concerning security, privacy, safety, and ethics. The paper delves into IoT security problems, requirements, and best practices by introducing IoT systems, architectures, and characteristics. It also discusses safety and ethical design issues while addressing challenges and remedies related to privacy.

According to Quach et al. [15], privacy conflicts arise from interactions enabled by digital technologies. They analyze how these technologies impact marketing and privacy issues in consumer-firm relationships. The authors present three principles and seven propositions using information from top managers and consumer informants. They develop a data strategy typology focusing on data monetization and data sharing, leading to four distinct types of businesses with varying responses to privacy concerns.

Easwara and Vu [16] explore factors influencing Voice Activated Personal Assistant (VAPA) use in public spaces via an online survey. Results show users are cautious about sharing private information, prefer VAPA use in remote locations, and reveal a positive correlation between VAPA usage likelihood and social acceptability.

Furthermore, e-Privacy regulations protect user privacy in the digital age. For instance, the General Data Protection Regulation (GDPR) has set a high standard for data protection, granting individuals significant control over their data. It has also influenced other jurisdictions to enact similar laws, such as the California Consumer Privacy Act (CCPA) in California and the African Union Convention on Cyber Security and Personal Data Protection (AUDPC). The AUDPC represents a significant step in harmonizing data protection regulations across African Union member states, focusing on the security of electronic transactions and personal data protection.

Additionally, the ePrivacy Directive, on the other hand, focuses specifically on the privacy of electronic communications. It prohibits any form of surveillance of electronic communications without the user's consent, which is particularly relevant in the context of overheard conversations for targeted advertising. However, these regulations also pose challenges for businesses, particularly those operating in multiple jurisdictions, as they must comply with different laws. Furthermore, the rapid advancement of technology often outpaces the development of regulations, creating a gap between what is technically possible and what is legally permissible.

In addition, the e-Privacy regulations provide essential user protections and pose business challenges. Stakeholders must understand these laws and their implications to navigate the complex landscape of e-Privacy effectively. Please refer to Table 1 for a summary of common e-Privacy laws.

To this end, unlike previous works, The novelty of this research lies in its unique exploration of the intersection between targeted advertising and voice recognition technology, specifically focusing on the phenomenon of overheard conversations. While previous studies have examined targeted advertising and voice recognition technology separately, this paper presents a promising investigation into how these two domains interact, particularly emphasizing user privacy and security implications.

## 3. Research methodology

The research methodology for this paper was designed to provide a comprehensive understanding of the intersection between targeted advertising, voice recognition technology, and user privacy. The methodology encompasses a multi-pronged approach, integrating literature review, theoretical analysis, and policy evaluation.The research design follows a systematic approach, guided by the principles outlined by Rahi in [22].

**Table 1**
Summary of Common e-Privacy Laws [17–21].

| Law | Jurisdiction | Key Provisions |
|---|---|---|
| GDPR | EU | Provides data subjects with significant control over their personal data. |
| CCPA | California, USA | It gives residents more control over the personal information that businesses collect about them. |
| PIPEDA | Canada | Governs how private sector organizations collect, use, and disclose personal information. |
| DPA 2018 | UK | Provides a comprehensive framework for data protection in the UK. |
| ePrivacy Directive | EU | Emphasizes the confidentiality of electronic communications and related traffic data. |
| AUDPC | African Union | It aims to establish a legal framework for cybersecurity and personal data protection within the African Union, promoting electronic transactions, personal data protection, and combating cybercrime. |

### 3.1. Literature review

The literature review served as the foundation for understanding the existing body of knowledge related to targeted advertising, voice recognition, and privacy concerns.

- Search Strategy: A comprehensive search was conducted using databases like IEEE Xplore, PubMed, Google Scholar, and Scopus. Keywords and Boolean operators were used to refine the search, focusing on terms like "targeted advertising," "voice recognition," "privacy," "security," and combinations thereof.
- Inclusion and Exclusion Criteria: Peer-reviewed articles, conference papers, and authoritative reports published within the last ten years were included. Non-peer-reviewed articles, opinion pieces, and studies lacking methodological rigor were excluded.
- Analysis: A thematic analysis was performed on the selected literature, categorizing findings into themes such as effectiveness, ethical concerns, technological evolution, and legal frameworks. Gaps and contradictions in the literature were also identified.

### 3.2. Theoretical analysis

The theoretical analysis aimed to explore the underlying mechanisms and ethical considerations of targeted advertising and voice recognition.

- Conceptual Framework: Key concepts were defined, and relevant theories were explored, such as data collection methods (e.g., cookies, device fingerprinting), user behavior analysis techniques, and ethical frameworks.
- Legal Analysis: A comparative legal analysis was conducted across different jurisdictions, examining laws like GDPR, CCPA, and ePrivacy Directive. The analysis focused on key provisions, compliance requirements, and enforcement mechanisms.

### 3.3. Policy evaluation and recommendations

This section involved an in-depth evaluation of existing policies, industry practices, and privacy-enhancing technologies.

- Data Sources: A wide range of sources was analyzed, including governmental policy documents, industry guidelines, technological white papers, and expert opinions.
- Evaluation Criteria: Policies and technologies were evaluated using a multi-dimensional framework, considering aspects like effectiveness in protecting privacy, compliance with legal requirements, transparency in data handling, and user control over personal information.
- Recommendations: Recommendations were formulated for various stakeholders, including specific policy amendments, technological implementations, and best practices for data handling.

The research methodology adopted in this paper offers a comprehensive and multi-faceted exploration of targeted advertising, voice recognition technology, and user privacy. By integrating a systematic literature review, in-depth theoretical analysis, and critical policy evaluation, the study provides valuable insights and practical recommendations.

## 4. The mechanism of targeted advertising

To understand the relationship between targeted advertising and security, it is essential first to explore the mechanics behind targeted advertising. This section delves into the process of online tracking and data collection, the analysis of user behavior for ad personalization, the role of third-party data brokers in the targeted advertising ecosystem,

and the ethical concerns associated with these practices.

- Online Tracking and Data Collection: The foundation of targeted advertising is built on the extensive tracking and collection of user data. This data is collected through several mechanisms, including cookies (small text files stored on users' devices), device fingerprinting (identifying unique device characteristics), and tracking pixels (invisible images embedded in websites and emails) [23]. Advertisers and marketers use these techniques to gather information about user behavior, interests, preferences, demographics, etc. As users browse the internet, engage with social media platforms, and use various online services, they leave behind a digital footprint [24].

  Information collected through these tracking methods can include website visits, search queries, page views, clicks, online purchases, and even the amount of time spent on specific pages. In addition to behavioral data, advertisers may also collect personal information such as age, gender, location, and device type. This wealth of data is invaluable for marketers as it provides insights into user habits, allowing them to create targeted advertising campaigns that resonate with specific user segments.

- Analyzing User Behavior for Ad Personalization: Once user data has been collected, it is processed and analyzed to create detailed profiles that facilitate ad personalization. Using algorithms and machine learning, patterns and trends in user behavior are identified, helping advertisers understand their target audience's preferences and needs [25]. These insights can be utilized to create highly targeted ad campaigns that cater to individual user interests. For example, an advertiser may target users who have recently searched for running shoes, visited fitness websites, or engaged with exercise-related content. By personalizing ads based on user behavior, advertisers aim to increase the likelihood of user engagement and conversion, ultimately enhancing the effectiveness and return on investment (ROI) of their marketing efforts [1].
- Role of Third-Party Data Brokers: The targeted advertising ecosystem is not solely driven by first-party data advertisers collect. Third-party data brokers play a significant role in aggregating, processing, and selling user data to advertisers and marketing agencies [26,27]. These data brokers collect information from various sources, including public records, social media platforms, and other online services. They then combine and analyze this data to create detailed user profiles that can be used for targeted advertising purposes [28]. Data brokers may also provide services such as data enhancement, wherein they supplement existing user profiles with additional information, or audience segmentation, where they group users into specific categories based on shared characteristics. By providing access to a vast pool of user data and insights, third-party data brokers contribute significantly to the success and sophistication of targeted advertising campaigns.
- Ethical Concerns in Targeted Advertising: Given the focus on user security and privacy, addressing the ethical concerns related to data collection, user profiling, and third-party data brokers is essential. The extensive collection and analysis of user data raise questions about user consent, data protection, and potential misuse of personal information. For instance, some users might be unaware of the extent to which their data is collected and used for targeted advertising purposes [3,29,30]. Moreover, the involvement of third-party data brokers in the targeted advertising ecosystem raises concerns about the transparency of data-sharing practices and the potential for unauthorised access to user data. These ethical concerns set the stage for exploring the potential implications of targeted advertising on user security and privacy and the possible connection between voice recognition technology and targeted ads.

In summary, targeted advertising relies on a complex process involving online tracking, data collection, user behavior analysis, the involvement of third-party data brokers, and ethical considerations associated with these practices. Understanding these mechanics is crucial for comprehending the potential implications of targeted advertising on user security and privacy and the possible connection between voice recognition technology and targeted ads. As technology evolves, ensuring transparency, user consent, and data protection becomes increasingly essential for maintaining the delicate balance between targeted advertising's benefits and the potential risks to user privacy and security.

### 4.1. Voice recognition and its role in advertising

Voice recognition technology can potentially revolutionize the targeted advertising landscape, offering new ways to personalize and deliver ads to users. However, integrating this technology raises significant privacy concerns and potential misuse scenarios. This section will explore the history and current state of voice recognition technology, its possible applications in targeted advertising, and the ethical considerations associated with its use.

- The Evolution of Voice Recognition Technology: The development of voice recognition technology dates back to the 1950s, with initial systems capable of recognizing only digits and limited vocabulary. One notable milestone in developing this technology was IBM's Shoebox system in the 1960s, which could remember 16 spoken words and the digits 0–9. Advances in artificial intelligence, machine learning, and natural language processing have since led to significant improvements in the accuracy and capabilities of voice recognition systems [31,32]. Today, voice recognition technology is widely integrated into devices and services such as smartphones, smart speakers, and virtual assistants like Siri, which was introduced by Apple in 2011, Alexa, and Google Assistant. These systems can process and analyze human speech, allowing devices to understand spoken language and respond accordingly. The growing accuracy and prevalence of voice recognition technology have opened new possibilities for its application in various fields, including targeted advertising [33,34].
- Potential Applications in Targeted Advertising: While voice recognition technology in targeted advertising is not yet widespread, several potential applications may emerge as the technology becomes more sophisticated. These applications could include:
  (a) Voice search: As voice search becomes more prevalent, advertisers may leverage voice recognition to analyze users' search queries and deliver relevant ads based on their interests and needs.
  (b) Contextual advertising: Voice recognition technology could be used to analyze the content of spoken conversations in real time, enabling advertisers to serve contextually relevant ads based on the topics discussed.
  (c) Sentiment analysis: By processing and understanding the emotional context of a user's speech, voice recognition technology could help advertisers target users based on their emotions or moods, resulting in more effective ad campaigns.
  (d) Personalized voice ads: Advertisers may develop voice ads tailored to individual users by leveraging voice recognition technology to analyze user preferences, demographic information, and other factors.
- Privacy Concerns and Potential Misuse: Integrating voice recognition technology into targeted advertising raises privacy concerns and potential misuse scenarios. Users may be unaware that their voice data is being collected and used for advertising, leading to questions about consent and transparency. Additionally, the widespread collection of voice data may create new risks associated with data breaches, unauthorised access, or malicious use [12,35].

Furthermore, the use of voice recognition technology in targeted advertising could potentially exacerbate existing privacy concerns related to online tracking and data collection. As advertisers access more granular and personal information about users, the risk of intrusive and invasive advertising practices may increase.

To address these concerns, it is essential to consider the ethical and legal frameworks surrounding using voice recognition technology in advertising and the importance of user consent and awareness. Potential regulations or guidelines that could be implemented to address these concerns include data minimization, requiring explicit user consent for voice data collection, or implementing strong encryption for stored voice data by understanding and addressing the potential privacy implications of integrating voice recognition technology into targeted advertising, a balance between effective marketing strategies and user security can be achieved.

## 5. Security implications of overheard conversations

The possibility of advertisers utilizing voice data from overheard conversations to serve targeted ads raises security implications. This section will explore how advertisers may access voice data, the legal frameworks and protections in place, and the importance of user consent and awareness in ensuring user security and privacy.

- How Advertisers May Access Voice Data: There are several potential ways through which advertisers could access voice data from users' conversations [36–40]:
  (a) Smart devices and virtual assistants: Smartphones, smart speakers, and virtual assistants like Siri, Alexa, and Google Assistant are constantly processing and analyzing voice data to provide relevant services. Although these devices are designed to record voice data only upon activation, the potential for accidental recording or unauthorised access cannot be ruled out.
  (b) Third-party applications: Some mobile applications may request access to the device's microphone to collect and analyze voice data. This data could be shared with advertisers directly or through third-party data brokers.
  (c) Eavesdropping through ad networks: Ad networks could potentially deploy tracking technologies to access and analyze voice data from users' devices. However, such practices would likely be illegal or against privacy regulations.
  (d) Hacking and data breaches: Voice data stored by device manufacturers, service providers, or third-party data brokers could be vulnerable to hacking or data breaches, exposing sensitive information to unauthorised parties, including advertisers.
- Legal Frameworks and Protections: Several legal frameworks and protections exist to safeguard user privacy and regulate the collection and use of voice data [17,41–45]:
  (a) General Data Protection Regulation (GDPR): The European Union's GDPR establishes strict guidelines for the collection, processing, and use of personal data, including voice data. Companies operating within the EU or targeting EU citizens must comply with GDPR requirements, which mandate user consent, data minimization, and data security.
  (b) California Consumer Privacy Act (CCPA): provides California residents with greater control over their personal information, including the right to know what data is collected, the right to opt out of the sale of personal information, and the right to delete personal information.
  (c) African Union Convention on Cyber Security and Personal Data Protection (AUDPC): The AUDPC is a significant legal framework within the African Union member states, focusing on the security of electronic transactions, personal data protection, and combating cybercrime. It sets guidelines for the collection, processing, storage, and sharing of personal data, including voice data, and encourages cooperation between member states in enforcing data protection laws.
  (d) Other national and regional regulations: Many countries have enacted data protection laws that address collecting and using personal data, including voice data. These laws vary in scope and stringency but aim to protect user privacy and security.
- User Consent and Awareness: User consent and awareness are crucial in ensuring voice data's security and privacy. Users should be informed about their voice data's collection, storage, and use and the potential risks associated with data breaches or unauthorised access. Consent mechanisms should be transparent, easy to understand, and allow users to make informed decisions about sharing their voice data. Examples of consent mechanisms include opt-in, opt-out, and granular consent options. Education and awareness campaigns can help users understand the implications of sharing voice data and empower them to take control of their privacy. Companies should be transparent about their data collection practices and provide users with accessible tools to manage their privacy settings.

In conclusion, the potential use of voice data from overheard conversations in targeted advertising raises several security implications. Understanding how voice data may be accessed, the existing legal frameworks and protections, and the importance of user consent and awareness are crucial for ensuring user security and privacy. Addressing these concerns can provide a balance between effective advertising strategies and user security can be achieved. Ensuring compliance with data protection regulations, promoting transparency, and empowering users with accessible privacy management tools are essential to maintaining this delicate balance. As technology evolves, stakeholders must remain vigilant and proactive in safeguarding user privacy and security in the face of ever-changing advertising landscapes.

### 5.1. *Strategies for protecting user privacy*

As targeted advertising continues to evolve and incorporate new technologies, such as voice recognition, it becomes increasingly important to implement strategies to protect user privacy. This section outlines privacy-enhancing technologies, policy recommendations for industry and regulators, and the significance of consumer awareness and education in safeguarding privacy.

- Privacy-Enhancing Technologies: Privacy-enhancing technologies (PET) are tools and solutions designed to protect user privacy while maintaining the functionality of digital services. Some PETs that can be used to protect user privacy in the context of targeted advertising include [46–49]:
  (a) Anonymization and pseudonymization: Techniques such as data masking and aggregation can be used to anonymize or pseudonymize personal data, reducing the risk of identification and privacy breaches.
  (b) Differential privacy: Differential privacy is a statistical method that allows data analysts to obtain valuable insights from datasets while preserving user privacy. This technique adds noise to the data, making it difficult to identify individual users while retaining the overall patterns and trends.
  (c) Private information retrieval: Private information retrieval (PIR) allows users to access specific data from a database without revealing which data they are interested in, thereby protecting their privacy.
  (d) Privacy-focused browser extensions: Browser extensions, such as uBlock Origin and Privacy Badger, can help users protect their privacy by limiting the amount of data collected and shared with advertisers.
- Policy Recommendations for Industry and Regulators

To ensure user privacy in the context of targeted advertising,

policymakers and regulators should consider implementing the following recommendations:

(a) Strengthen data protection regulations: Policymakers should enforce and update data protection regulations to account for emerging technologies and potential privacy threats.
(b) Promote transparency and user control: Regulators should require companies to be transparent about their data collection practices and provide users with accessible tools to manage their privacy settings.
(c) Encourage the adoption of privacy-enhancing technologies: Governments and industry organizations should incentivize using PETs and invest in research and development to create more advanced privacy solutions.
(d) Establish industry best practices: Industry associations, such as the Interactive Advertising Bureau (IAB), should develop and promote best practices for data collection, storage, and use in targeted advertising, emphasizing user privacy and security.

- Consumer Awareness and Education: Consumer awareness and education are crucial for ensuring user privacy in the face of targeted advertising. Users can make informed decisions about their privacy settings and online behavior by understanding the potential risks and implications of sharing their data. Initiatives to increase consumer awareness and education can include:
  (a) Public awareness campaigns: Governments and non-profit organizations, such as the Electronic Frontier Foundation (EFF), can launch public awareness campaigns to educate users about the potential privacy risks associated with targeted advertising and voice recognition technology.
  (b) Clear privacy policies: Companies should provide users with clear and concise privacy policies, highlighting their data collection and usage practices in a manner that is easy to understand.
  (c) Educational resources: Providing accessible resources, such as guides and tutorials from organizations like the Center for Democracy & Technology (CDT), can help users navigate privacy settings and make informed choices about their online activity.

In summary, protecting user privacy in targeted advertising requires a multi-pronged approach, encompassing privacy-enhancing technologies, policy recommendations for industry and regulators, and consumer awareness and education. Through the implementation of these strategies, a balance can be achieved between the benefits of targeted advertising and the need to safeguard user privacy and security.

## 6. Conclusion

In conclusion, this paper has explored the various aspects of targeted advertising, its evolution, and the potential implications of incorporating voice recognition technology. The paper has highlighted the benefits and challenges associated with targeted advertising, such as improved user experience, increased ad relevance, and concerns over user privacy and security. As targeted advertising becomes more sophisticated, it is essential to consider the ethical and legal implications of new technologies, such as voice recognition, and their potential impact on user privacy.

The paper has examined the history and current state of voice recognition technology and the potential applications and concerns associated with its use in targeted advertising. Furthermore, it has delved into the security implications of overheard conversations, emphasizing the importance of user consent, awareness, and legal frameworks in protecting user privacy.

Strategies for protecting user privacy have been outlined, focusing on privacy-enhancing technologies, policy recommendations for industry and regulators, and consumer awareness and education. The importance of collaboration between various stakeholders and the continuous monitoring and evaluation of privacy protection strategies has also been emphasized.

In the face of rapid technological advancements and evolving advertising landscapes, it is crucial to balance the effectiveness of targeted advertising and the need to safeguard user privacy and security. As new technologies emerge, stakeholders must remain vigilant and proactive in addressing potential privacy risks and ensuring compliance with data protection regulations. Through promoting transparency, empowering users with accessible privacy management tools, and fostering a collaborative approach to privacy protection, it is possible to create an advertising ecosystem that benefits businesses and consumers without compromising the fundamental right to privacy.

## Funding statement

Not applicable.

## Additional information

No additional information is available for this paper.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

No data has been used.

## References

[1] Y. Luzon, R. Pinchover, E. Khmelnitsky, Dynamic budget allocation for social media advertising campaigns: optimization and learning, Eur. J. Oper. Res. 299 (1) (2022) 223–234.
[2] B. Tk, C.S.R. Annavarapu, A. Bablani, Machine learning algorithms for social media analysis: a survey, Comput. Sci. Rev. 40 (2021), 100395, https://doi.org/10.1016/j.cosrev.2021.100395.
[3] A.C. Plane, E.M. Redmiles, M.L. Mazurek, M.C. Tschantz, Exploring user perceptions of discrimination in online targeted advertising, in: Proceedings of the USENIX Security Symposium, 2017, pp. 935–951.
[4] B.E. Elbaghazaoui, M. Amnai, Y. Fakhri, Voice recognition and user profiling. Advances in Cybersecurity, Cybercrimes, and Smart Emerging Technologies, Springer, 2023, pp. 223–233.
[5] "Can your phone hear your conversations? (Yes, But Here's How)." https://www.spiralytics.com/blog/mobile-ads-can-phone-hear-conversations-infographic/ (accessed Apr. 18, 2023).
[6] S. Englehardt, A. Narayanan, Online tracking: a 1-million-site measurement and analysis, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, 2016, pp. 1388–1401, https://doi.org/10.1145/2976749.2978313.
[7] A. Lambrecht, C. Tucker, Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads, Manag. Sci. 65 (7) (2019) 2966–2981.
[8] X. Huang, J. Baker, R. Reddy, A historical perspective of speech recognition, Commun. ACM 57 (1) (2014) 94–103.
[9] L. Wu, F. Morstatter, K.M. Carley, H. Liu, Misinformation in social media: definition, manipulation, and detection, ACM SIGKDD Explor. Newsl. 21 (2) (2019) 80–90. Available, https://www.nytimes.com/2016/11/21/technology/fact.
[10] U. Iqbal et al., "Your echos are heard: tracking, profiling, and ad targeting in the Amazon smart speaker ecosystem," arXiv Prepr. arXiv2204.10920, 2022.
[11] V. Jesus, H.J. Pandit, Consent receipts for a usable and auditable web of personal data, IEEE Access 10 (2022) 28545–28563, https://doi.org/10.1109/ACCESS.2022.3157850.
[12] L.H. Acosta, D. Reinhardt, A survey on privacy issues and solutions for voice-controlled digital assistants, Pervasive Mob. Comput. 80 (2022), 101523.
[13] Y. Himeur, S.S. Sohail, F. Bensaali, A. Amira, M. Alazab, Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives, Comput. Secur. (2022), 102746.
[14] H.F. Atlam, G.B. Wills, IoT Security, Privacy, Safety and Ethics, Springer International Publishing, 2020, https://doi.org/10.1007/978-3-030-18732-3_8.

[15] S. Quach, P. Thaichon, K.D. Martin, S. Weaven, R.W. Palmatier, Digital technologies: tensions in privacy and data, J. Acad. Mark. Sci. 50 (6) (2022) 1299–1323, https://doi.org/10.1007/s11747-022-00845-y.
[16] A.E. Moorthy, K.P.L. Vu, Privacy concerns for use of voice activated personal assistant in the public space, Int. J. Hum. Comput. Interact. 31 (4) (2015) 307–335.
[17] M. Bouke, A. Abdullah, S. ALshatebi, H.E. Atigh, and K. Cengiz, "African union convention on cyber security and personal data protection: challenges and future directions," arXiv Prepr. arXiv2307.01966, vol. 56, no. 1, pp. 164–192, Jul. 2023. Available: http://arxiv.org/abs/2307.01966.
[18] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, B. Stiller, Landscape of IoT security, Comput. Sci. Rev. 44 (2022), 100467, https://doi.org/10.1016/j.cosrev.2022.100467.
[19] L.M. Austin, Reviewing pipeda: control, privacy and the limits of fair information practices, Can. Bus. LJ 44 (2006) 21.
[20] P. Regulation, General data protection regulation, Intouch 25 (2018) 1–5.
[21] H. Li, L. Yu, W. He, The impact of GDPR on global technology development, J. Glob. Inf. Technol. Manag. 22 (1) (2019) 1–6. Taylor & Francis.
[22] S. Rahi, Research design and methods: a systematic review of research paradigms, sampling issues and instruments development, Int. J. Econ. Manag. Sci. 6 (2) (2017) 1–5.
[23] D.H. Granello, J.E. Wheaton, Online data collection: strategies for research, J. Couns. Dev. 82 (4) (2004) 387–393.
[24] A. Karaj, S. Macbeth, R. Berson, and J.M. Pujol, "Whotracks. me: monitoring the online tracking landscape at scale," CoRR, abs/1804.08959, 2018.
[25] B. Gao, L. Huang, Understanding interactive user behavior in smart media content service: an integration of TAM and smart service belief factors, Heliyon 5 (12) (2019) e02983.
[26] T.M.C. Jai, N.J. King, Privacy versus reward: do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? J. Retail. Consum. Serv. 28 (2016) 296–303.
[27] L. Roderick, Discipline and power in the digital age: the case of the US consumer data broker industry, Crit. Sociol. 40 (5) (2014) 729–746.
[28] U. Reviglio, The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview, Internet Policy Rev. 11 (3) (2022) 1–27.
[29] S.L.S. Nwachukwu, S.J. Vitell, F.W. Gilbert, J.H. Barnes, Ethics and social responsibility in marketing: an examination of the ethical evaluation of advertising strategies, J. Bus. Res. 39 (2) (1997) 107–118.
[30] I. Lefter, Ethics and advertising-Female targeted advertisement and the ethical concerns of practitioners and scholars, J. Ethics Soc. Stud. 2 (2) (2018) 33–42.
[31] "IBM100 - pioneering speech recognition." https://www.ibm.com/ibm/history/ibm100/us/en/icons/speechreco/ (accessed Apr. 19, 2023).
[32] S. Davis, P. Mermelstein, Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences, IEEE Trans. Acoust. 28 (4) (1980) 357–366.
[33] N. Jain, S. Rastogi, Speech recognition systems-a comprehensive study of concepts and mechanism, Acta Inform. Malaysia 3 (1) (2019) 1–3.
[34] C. Shan, J. Wang, Y. Zhu, The evolution of artificial intelligence in the digital economy: an application of the potential dirichlet allocation Model, Sustainability 15 (2) (2023) 1360.
[35] K. Xu, S. Chan-Olmsted, F. Liu, Smart speakers require smart management: two Routes from user gratifications to privacy settings, Int. J. Commun. 16 (2022) 23.
[36] N. Malkin, J. Bernd, M. Johnson, S. Egelman, What can't data be used for?' Privacy expectations about smart tvs in the us, in: Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK, 2018.
[37] A. Ross, S. Banerjee, A. Chowdhury, Security in smart cities: a brief review of digital forensic schemes for biometric data, Pattern Recognit. Lett. 138 (2020) 346–354.
[38] B. Sander, Freedom of expression in the age of online platforms: the promise and pitfalls of a human rights-based approach to content moderation, Fordham Int'l LJ 43 (2019) 939.
[39] F. Bradley, Representation of libraries in artificial intelligence regulations and implications for ethics and practice, J. Aust. Libr. Inf. Assoc. 71 (3) (2022) 189–200.
[40] G. Mazurek, K. Małagocka, Perception of privacy and data protection in the context of the development of artificial intelligence, J. Manag. Anal. 6 (4) (2019) 344–364.
[41] A. Tamò-Larrieux, S. Tamò-Larrieux, Seyfried, Designing For Privacy and Its Legal Framework, 12, Springer, 2018.
[42] M. Bartlett, Beyond privacy: protecting data interests in the age of artificial intelligence, Law, Technol. Humans 3 (1) (2021) 96–108.
[43] M. Namara, D. Wilkinson, B.M. Lowens, B.P. Knijnenburg, R. Orji, R.L. Sekou, Cross-cultural perspectives on eHealth privacy in Africa, in: Proceedings of the 2nd African Conference for Human Computer Interaction: Thriving Communities, 2018, pp. 1–11.
[44] R.H. Weber, Internet of Things–New security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30.
[45] A. Union, African Union convention on cyber security and personal data protection, Afr. Union 27 (2014).
[46] Y. Shen, S. Pearson, Privacy enhancing technologies: a review, Hewlet Packard Dev. Company. Dispon. (2011). https://bit.ly/3cfpAKz.
[47] Y. Wang, Privacy-enhancing technologies. Handbook of Research on Social and Organizational Liabilities in Information Security, IGI Global, 2009, pp. 203–227.
[48] S. Fischer-Hbner, S. Berthold, Privacy-enhancing technologies. Computer and Information Security Handbook, Elsevier, 2017, pp. 759–778.
[49] N. Kaaniche, M. Laurent, S. Belguith, Privacy enhancing technologies for solving the privacy-personalization paradox: taxonomy and survey, J. Netw. Comput. Appl. 171 (2020), 102807.