Smart Speakers Privacy Breach

Dipansh Garg (ID: 222194683)
Report
Deakin University
Melbourne, Australia
s222194683@deakin.edu.au

***Abstract*—This research report examines the significant privacy breach involving smart speakers from Amazon Echo, Google Home, and Apple Siri, where human reviewers systematically accessed users' private voice recordings without adequate user consent. The investigation reveals how thousands of auditors and contractors processed recordings captured through both intentional interactions and accidental recordings triggered by false wake word activations. Exposed data included sensitive personal conversations, confidential business information, and domestic exchanges that users reasonably expected to remain private. Analysis demonstrates how this privacy breach stemmed from fundamental issues in voice recording quality assurance protocols, wake word technology limitations, and insufficient data protection measures. The paper draws on interdisciplinary research spanning technical performance, user behavior, privacy perceptions, and legal frameworks to provide a comprehensive understanding of the incident. While users develop personalized relationships with their voice assistants, often treating them as 'para-friends' as identified by Mckie et al. The report identifies technical, procedural, and regulatory approaches that could have prevented unauthorized human review of sensitive audio data, and provides actionable recommendations for both corporate data collection policies and consumer privacy management strategies. These findings demonstrate the critical need for balancing the convenience of voice-activated technologies with robust privacy safeguards in an increasingly smart speaker-dependent ecosystem. These findings demonstrate the critical need for balancing the convenience of voice-activated technologies with robust privacy safeguards in an increasingly smart speaker-dependent ecosystem.**

Keyword: Smart speakers, voice assistants, privacy breach, voice recordings, user consent, wake word detection, data protection, Amazon Alexa, Google Assistant, Apple Siri, IoT security, privacy compliance, consumer protection, audio surveillance, human reviewers.

I. Introduction

A. Background on Smart Speakers and Voice Assistants

Smart speakers have rapidly transformed from novelty gadgets to ubiquitous household devices, creating new patterns of human-computer interaction through conversational interfaces [1]. These voice-activated systems, primarily Amazon Echo (Alexa), Google Home (Google Assistant), and Apple HomePod (Siri), serve as the central interface for burgeoning smart home ecosystems while providing convenient access to information, entertainment, and services through natural language interaction.

B. Market Penetration and Consumer Adoption

Smart speakers have achieved remarkable market penetration across diverse demographics. Studies indicate high overall awareness (>80%) of Amazon Echo, Google Home, and Apple Siri, with adoption primarily focused on basic tasks such as music playback, setting reminders, and making calls [1]. The technology has proven especially appealing to young, tech enthusiasts who demonstrate a greater willingness to experiment with advanced features, though privacy concerns and perceived usefulness remain key barriers to deeper engagement [2].

C. Privacy Expectations and Reality Gap

Consumers have generally maintained an expectation that their interactions with smart speakers remain private or, at minimum, are processed solely by automated systems. The devices' always-listening architecture that is necessary for detecting wake words like "Alexa," "Hey Google," or "Hey Siri" has raised inherent privacy questions, but many users assumed that only explicitly triggered voice recordings were stored or analyzed [3]. This perception contrasts sharply with the reality uncovered by investigations into these companies' practices. Rather than purely algorithmic processing, thousands of human reviewers were systematically accessing user recordings, including conversations captured through accidental activations, to improve voice recognition systems. This previously undisclosed human review process represented a significant gap between consumer privacy

expectations and actual corporate practices, highlighting severe deficiencies in user consent mechanisms.

D. Scope of the Research

This report examines the privacy breach involving employee access to smart speaker recordings, analyzing when and how it occurred, who was affected, and what technical and procedural vulnerabilities enabled it. Beyond documenting the breach, the research evaluates preventive measures, defense strategies, and mitigation approaches applicable to both corporations and consumers. The report concludes with recommendations for promoting IoT security awareness and enhancing privacy protections in voice-enabled technologies.

E. Report Structure

This report is organized as follows: Section II provides background and literature review on voice assistant technology and privacy research, Section III examines the scope and impact of the privacy breach, detailing the affected systems, data types, and stakeholders. Section IV provides a technical and procedural analysis of how the breach occurred, including wake word failures and data handling procedures. Section V assesses the preventability of the breach from both technical and procedural perspectives. Section VI outlines defense strategies available to both technical systems and policy frameworks. Section VII discusses corporate mitigation measures implemented in response to the breach. Section VIII presents consumer protection strategies and practical privacy controls. Section VII addresses the broader need for IoT security awareness and education. Section X explores future directions in voice assistant privacy, including emerging technologies and evolving regulations. Finally, Section XI concludes with key findings and recommendations for balancing innovation with privacy protection in voice-activated technologies.

II. Background and Literature Review

A. Market Growth and Adoption Patterns

The voice assistant market has experienced exponential growth, with projections indicating the Indian market alone could expand at approximately 270% per annum, potentially exceeding USD 30 billion by 2030 [1]. This robust adoption reflects consumers' embrace of voice-based artificial intelligence for tasks ranging from playing music and setting reminders to controlling connected home devices [4]. Figure 1 reveals that smart speaker ownership is highest among younger demographics, with ownership rates declining and disinterest increasing with age. Based on 45,883 responses collected in late 2021 from US adults 18+.

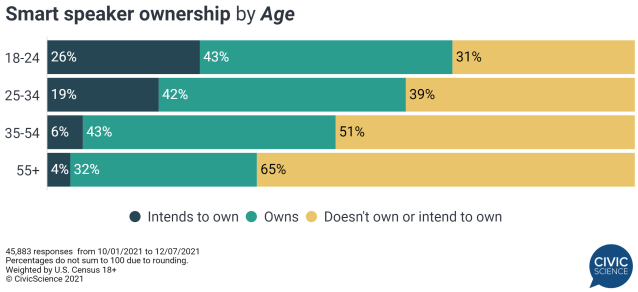

Fig. 1: Appeal of smart speakers to various age ranges [5]

1) B. Research Frameworks and User Behavior: Minder et al. [6] developed a comprehensive framework identifying nine thematic clusters across voice assistant research, spanning from technical performance to privacy concerns and assisted living applications. Their analysis reveals four principal research streams such as conceptual foundations, systemic challenges, efficiency applications, and specialized use cases, highlighting the cross-disciplinary nature of voice assistant development and adoption.

Tabassum et al. [3] found that users imagine both familiar functions (calendar reminders, recipe suggestions) and novel context-aware features (automatic reservations, purchases) as valuable services that voice assistants could provide. Their research also revealed that existing smart speaker owners were more likely to consent to conversation sharing, suggesting that familiarity with the technology influences privacy risk assessment.

2) C. Voice Interface Design and Usability: Zwakman et al. [7] found that traditional usability metrics inadequately capture the voice interface experience, developing a specialized Voice Usability Scale (VUS) that measures three critical dimensions being general usability, affective experience, and recognizability. Their research suggests that voice interfaces present unique challenges compared to graphical interfaces, requiring specialized evaluation methods.

3) D. Market Dominance and Competition Concerns: The dominance of major technology companies in this space, Amazon, Google, and Apple, has created what the European Commission's IoT sector inquiry identified as concerns around defaults, data accumulation, and interoperability [1]. These market leaders have established powerful ecosystems that extend the capabilities of their

voice assistants while deepening their access to consumer data, potentially engaging in what Morozovaite terms "hypernudging" as dynamically personalized steering of consumers that could amount to anticompetitive self-preferencing [1].

4) E. User Personification and Privacy Perceptions: Mckie et al. [8] found that long-term users develop complex relationships with their voice assistants, often personifying them with human-like traits (e.g., "Uncle Google," "Auntie Alexa"). This personification creates a paradoxical situation where users simultaneously develop intimate relationships with their devices while being unaware that actual humans may review their private utterances. The same study noted that voice interfaces fundamentally alter information search behavior, with results delivered sequentially rather than as browsable lists, further affecting users' expectations about how their data is handled.

5) F. Privacy Research Evolution: Maccario and Naldi [9] found that privacy concerns appear in under 3% of Amazon Echo reviews, suggesting that many users either overlook privacy risks or consider them inconsequential compared to functionality. Among those privacy-related mentions, approximately 70% are positive, though a substantial minority expresses negative sentiment. This polarization indicates that negative privacy concerns do not necessarily translate into lower overall satisfaction with smart speaker products.

Tabassum et al. [3] directly examined the privacy-utility tradeoff, finding that comfort with voice assistant services and perceived usefulness positively correlated with willingness to share conversational data, while perceived sensitivity of conversations strongly deterred sharing.

III. Scope and Impact

A. Targeted Systems and Data

The privacy breach centered on the cloud-based voice processing infrastructure supporting three major smart speaker platforms being Amazon Echo (Alexa), Google Home (Google Assistant), and Apple HomePod/iPhone (Siri). Each system employs a similar technical architecture: devices continuously monitor ambient audio for wake words, after which recordings are transmitted to cloud servers for processing, response generation, and quality assurance review.

1) Voice Recording Storage Systems: All three companies maintained extensive voice recording storage systems that retained user interactions for varying periods. These systems enabled "continuous listening" functionality necessary for wake word detection while generating massive datasets of user utterances. Amazon's storage infrastructure was particularly extensive, as the company employed thousands of human reviewers who required access to historical recordings.

The voice data typically included:

- Audio recordings of user commands and queries
- Timestamps and device identifiers
- User account information (though sometimes pseudonymized)
- Contextual metadata about interactions

Hyma et al. [10] note that these platforms implemented a "wake-word filter" as the first line of privacy protection, but this mechanism proved insufficient due to frequent false activations that triggered recording without explicit user intent. Their research proposes a modular architecture layering a wake-word filter, a privacy "word bank" for sensitive terms, and a user preference engine that could block or anonymize utterances containing private information before they reach cloud services [10].

Tabassum et al. [3] identified additional user concerns about always-listening voice assistants, including potential misperformance, irrelevant suggestions, loss of control, conversational interruptions, and security vulnerabilities. Their research underscores the importance of transparent consent models, fine-grained controls, and clear value propositions to foster trust in voice recording and processing systems.

2) Data Processing Infrastructure: The cloud infrastructure processing these recordings included multiple systems:

- **Automatic Speech Recognition (ASR)** systems that converted audio to text
- **Natural Language Understanding (NLU)** components that interpreted user intent
- **Response generation systems** that produced appropriate answers
- **Quality assurance platforms** that facilitated human review of recordings

Figure 2 provides a visual understanding of the architecture discussed so far in this section, beginning from user verbal input: It was this last component, **the quality assurance platforms**, that exposed user data to employee access. These systems typically provided reviewers with audio playback capabilities, transcription tools, and classification interfaces for improving machine learning models. The review process was essential for improving functionality, but as Barricelli et al. [11] ob-

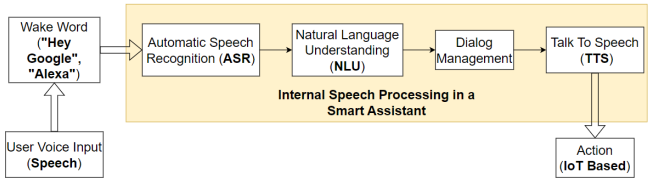

Fig. 2: A general architecture of the cloud-based voice processing system

serve, optimizing user interaction depends on balancing error reduction with privacy considerations, particularly when designing conversational interfaces for IoT ecosystems.

Mckie et al. [8] highlight how users develop specific strategies to interact with voice assistants based on perceived ”personalities” of the systems. This personification affects information-seeking behavior and creates expectations about how data is processed. The discovery that human reviewers analyzed these seemingly private interactions represents a significant breach of the tacit social contract established between users and their personified assistants.

3) Types of Data Exposed: The data exposed through these systems was particularly sensitive due to its audio nature and the intimate contexts in which smart speakers operate. Exposed information included:

- Personal conversations captured through accidental recordings
- Voice patterns that could potentially identify speakers
- Background discussions unrelated to device interactions Alzate et al. [12] identified particularly sensitive keywords in exposed recordings, including ”data,” ”record,” and ”listen,” which correlated with stronger negative sentiment in social media discussions that included:
- Confidential business information captured during office use, raising legal concerns similar to those discussed by Cook and Mavrova Heinrich [13] regarding the ethical obligations and privacy considerations that apply when handling sensitive information
- Domestic disputes and private household interactions
- Interactions with children and other vulnerable users

This extensive data exposure occurred largely without users’ meaningful awareness or explicit consent, despite being integral to the companies’ quality improvement processes. The vulnerability of such data has implications beyond personal privacy. In commercial settings, Buhalis and Moldavska [4] highlight how voice assistants in hospitality environments could expose sensitive guest information, though they also note potential benefits for operational efficiency and service enhancement.

Minder et al. [6] argue that addressing such privacy challenges requires an ecosystem approach that integrates technical safeguards, clear communication, and appropriate regulatory frameworks. Their conceptual framework emphasizes the need for interdisciplinary efforts to develop secure, privacy-preserving voice assistant solutions that users perceive as both safe and beneficial.

B. Affected Stakeholders

The privacy breach affected multiple stakeholder groups, each experiencing different impacts from the exposure of voice recordings to human reviewers.

1) Consumer Impact Assessment: Everyday consumers constituted the largest affected group, with millions of smart speaker users unwittingly having their voice interactions and accidental recordings reviewed by employees. For these users, the impact varied based on several factors:

- **Usage patterns:** Heavy users with frequent device interactions faced greater exposure
- **Conversation sensitivity:** Users discussing personal matters near devices experienced greater privacy invasion
- **Awareness levels:** Those with lower privacy literacy were less likely to understand risks or implement protections [14].

A study conducted in 2021 by Pitardi and Marriott [15] reveals that consumers develop complex relationships with voice assistants, treating them as ”para-friends” while often underestimating privacy risks. Their study found that social attributes such as social presence and social cognition significantly drive trust, while privacy concerns negatively affect attitudes but not necessarily trust or continued use. This paradoxical relationship helps explain why many users continued using smart speakers despite potential privacy concerns.

Zwakman et al. [7] further illuminate how users experience voice interfaces differently from traditional interfaces, with their Voice Usability Scale identifying three key dimensions: general usability, affective experience, and recognizability. The affective dimension is particularly relevant to privacy considerations, as it encompasses the emotional and trust-based aspects of

the user-device relationship that may be compromised by unauthorized human review of recordings.

Molinillo et al. [16] further complicate this picture by showing that emotional value and performance expectancy are consistently strong drivers of continuance intention with voice assistants, while privacy risk shows no direct effect on usage intention. Their research indicates that less innovative users are more sensitive to quality value, while experienced users respond more to social value features.

2) Business Users and Confidentiality Implications: Organizations deploying smart speakers in workplace environments faced distinct risks from the privacy breach. For these stakeholders, exposed audio potentially included:

- Strategic business discussions caught by accidental activations
- Confidential client information
- Proprietary processes and trade secrets
- Employee personal information

As Lyu et al. [14] demonstrate in their research on privacy protection behavior in contactless digital services, users often disengage from protecting their privacy even when they perceive risk. Their study found that privacy invasion increases both privacy fatigue and privacy literacy, with higher privacy fatigue increasing disengagement while higher privacy literacy decreases it, insights directly applicable to organizational smart speaker deployment.

The privacy implications extend to professional fields where confidentiality is legally mandated. E.g., Cook and Mavrova Heinrich [13] examine how attorneys must balance technological adoption with ethical duties of competence, communication, and confidentiality. Their framework for "AI-ready" legal practices emphasizes the need for robust vendor vetting, minimal data exposure, and firm-wide privacy policies that are considerations equally relevant for organizations using voice assistants in sensitive environments.

IV. Technical and Procedural Analysis

A. How the Privacy Breach Occurred

The privacy breach involving employee access to smart speaker recordings stemmed from a combination of technical limitations, operational requirements, and insufficient transparency about human review processes. Bolton et al. [17] identified four critical risk zones in the voice assistant pipeline where privacy vulnerabilities emerged: microphone capture, local wake-word filtering, cloud processing, and third-party skill execution.

1) Wake Word Detection Failures: At the heart of the privacy issue were false activations of the wake word detection system. Smart speakers continuously listen for specific trigger phrases ("Alexa," "Hey Google," "OK Siri") but are designed to only transmit audio to the cloud after detecting these phrases. However, as documented by multiple investigations, the wake word detection systems frequently misinterpreted ambient sounds, conversations, or media content as wake words, inadvertently triggering recording and transmission.

Cheng and Roedig [18] categorized these wake word vulnerabilities under "Access Control" threats, noting that current wake word technology suffers from both false positives (triggering when no wake word was spoken) and adversarial exploitations (where deliberate audio patterns can trigger activation). Their survey highlighted how these algorithmic triggers frequently failed to distinguish between genuine commands and background conversations or ambient noise.

According to Edu et al. [19], microphone hijacking could occur through feedback loops where speakers inadvertently amplified wake-word sound waves back into the device's microphone, creating unexpected activations. This technical vulnerability was compounded by users' unawareness of when recordings were being transmitted, as visual indicators on devices were often subtle or overlooked.

2) Quality Assurance Requirements: The business imperative to improve voice recognition accuracy drove companies to implement human review of recorded interactions. This manual review protocol involved thousands of contractors and employees who listened to voice recordings to:

- Verify speech-to-text conversion accuracy
- Annotate user intentions and commands
- Identify patterns in accidental activations
- Improve natural language understanding
- Train machine learning models for better recognition

Sharif and Tenbergen [20] identified always-listening microphones as one of six main vulnerability types in smart home voice assistants. Their research showed that the combination of continuous listening capability with cloud transmission created opportunities for excessive data collection beyond what users had reasonably authorized.

The quality control processes operated on a massive scale. According to reports, Amazon employed thousands of auditors globally to review Echo recordings, with each reviewer potentially processing hundreds of

audio clips daily. This industrial-scale audio transcription operation remained largely unknown to device owners, who had no clear mechanism to know which of their interactions were subjected to human review.

3) Accidental and Background Recordings: The most concerning aspect of the privacy breach involved accidental recordings that captured sensitive personal information. These unintended recordings occurred through several mechanisms:

- **False wake word activations**: Ambient sounds misinterpreted as wake words
- **Media-triggered activations**: Television advertisements or programs containing phrases similar to wake words
- **Background conversations**: Private discussions captured during legitimate device use
- **Continuous recording errors**: Technical malfunctions causing extended recording beyond command completion

Bolton et al. [17] highlighted how acoustic injection attacks could deliberately exploit these vulnerabilities, with ultrasonic "Dolphin" commands embedded in music bypassing human detection yet invoking unauthorized actions on voice assistants. While the privacy breach primarily involved accidental rather than malicious activations, the same technical vulnerabilities enabled both scenarios.

Tsourakas et al. [21] observed that users adapted their query phrasing for reliability, developing specific patterns of interaction to minimize misunderstandings. However, this adaptation did not protect against accidental activations caused by conversational fragments that happened to match wake word patterns.

B. Data Handling Procedures

Once recordings were captured, several data handling processes exacerbated the privacy implications of the breach, including inadequate anonymization, loose access controls, and unclear data retention policies.

1) Anonymization Techniques and Limitations: Companies attempted to anonymize voice recordings before employee review, typically by disassociating recordings from specific user accounts and applying pseudonymization techniques. However, these measures proved inadequate for several reasons:

- Voice data inherently contains biometric identifiers
- Spoken content often included personally identifiable information
- User identifiers and contextual metadata remained accessible in some systems
- Reviewers could hear background conversations containing names or sensitive details

Maccario and Naldi [22] conducted a systematic literature review of privacy issues in smart speakers, documenting vulnerabilities in anonymization practices. Their taxonomy of privacy concerns highlighted how voice data encryption measures frequently failed to prevent employee access to identifiable information.

2) Employee Access Controls: The systems providing employee access to voice recordings exhibited significant flaws in access control mechanisms. According to investigations, contractors and employees could:

- Access thousands of recordings daily
- Review recordings from potentially any user
- Hear complete utterances, including accidental activations
- In some cases, correlate recordings with approximate device location data

Singh et al. [23] identified multi-tenant isolation breach as a critical vulnerability in cloud-based systems, noting how shared access to data processing environments could compromise privacy. Their research highlighted the inadequacy of existing cloud processing security measures for protecting sensitive voice data.

3) Data Retention and Transmission Protocols: The data transmission protocols between devices and cloud servers, while generally encrypted, still created privacy exposures:

- Voice recordings were stored for extended and often unspecified periods
- Storage duration policies were not clearly communicated to users
- Limited user control over data deletion and retention
- Inconsistent implementation of automatic deletion features

Vardakis et al. [24] categorized these issues under data breach vulnerabilities, emphasizing how plaintext telemetry uploads and extended storage durations created unnecessary privacy risks. Their research recommended encryption and key management solutions, including TLS 1.3 for cloud-device channels and hardware security modules for key storage, to mitigate these risks.

Edu et al. [19] noted that even when voice content was anonymized, continuous metadata collection (timestamps, device IDs) enabled user profiling. This meant that even with partial anonymization efforts, the data transmission protocols still enabled potentially invasive analysis of user behaviors.

V. Preventability Assessment

A. Technical Preventability

From a technical perspective, the privacy breach involving employee access to recordings could have been substantially mitigated through several approaches that were technologically feasible but not implemented.

1) On-Device Processing Alternatives: The most significant technical prevention measure would have been expanding on-device speech processing capabilities. Bolton et al. [17] specifically recommended on-device processing to reduce cloud exposure as a primary mitigation strategy. By processing voice commands locally rather than transmitting them to cloud servers, the opportunities for human review would have been dramatically reduced.

Several technical approaches were viable:

- **Edge computing**: Processing basic commands entirely on the device
- **Selective cloud processing**: Only sending complex queries to the cloud
- **Improved algorithms**: Enhancing wake word detection accuracy to reduce false positives
- **Differential privacy techniques**: Applying noise to data before transmission to protect individual privacy

Cheng and Roedig [18] emphasized the urgent need for on-device speech recognition and robust wake-word spoofing detection to limit unintended data capture. Their survey documented how emerging edge AI capabilities could enable private voice processing while maintaining core functionality.

Singh et al. [23] proposed secure boot and attestation mechanisms utilizing TPM-backed firmware verification before establishing cloud sessions, which could have ensured devices only transmitted data under secure, authorized conditions.

2) Secure Enclaves and Federated Learning: For scenarios where cloud processing remained necessary, several technical safeguards could have prevented unauthorized human access:

- **Secure enclaves**: Processing voice data in hardware-secured environments inaccessible to employees
- **Federated learning**: Training speech recognition models across user devices without centralizing sensitive recordings
- **Voice authentication**: Using biometric verification to ensure recordings came from authorized users only
- **False positive reduction**: Implementing secondary verification before cloud transmission

These approaches represent a shift from trust-based to verification-based security models. As Vardakis et al. [24] noted, hardware security modules for key storage coupled with advanced encryption would have significantly reduced exposure risks even when cloud processing was required.

B. Procedural and Policy Preventability

Beyond technical solutions, procedural and policy changes could have prevented or minimized the privacy breach.

1) Informed Consent and Transparency: The most significant procedural failure was the lack of explicit, informed consent for human review of recordings. Effective consent mechanisms would have included:

- **Explicit permission**: Clearly asking users to opt into human review
- **Granular consent options**: Allowing users to choose which types of recordings could be reviewed
- **Privacy policy disclosures**: Transparent documentation of review practices
- **Ongoing notification**: Indicators when recordings were selected for human review

Maccario and Naldi [22] highlighted the evolution of privacy research on smart speakers, noting that from 2017 through 2021, research publications on smart speaker privacy grew at a compound annual rate of 63.45%, indicating growing recognition of these issues even as the implementation of proper consent mechanisms lagged.

2) Regulatory Compliance Frameworks: Stronger adherence to existing regulatory frameworks could have prevented the privacy breach:

- **GDPR compliance**: Following European data protection requirements for clear consent
- **CCPA adherence**: Implementing California privacy requirements
- **FTC regulations**: Following U.S. Federal Trade Commission guidelines on privacy disclosures
- **Industry standards**: Adopting emerging best practices for voice assistant privacy

Sharif and Tenbergen [20] recommended two-factor voice authentication, sandboxed skill execution, and clear user guidance on device hardening, representing an integrated approach to procedural safeguards.

Tsourakas et al. [21] found that many users underutilized voice assistant applications specifically due to perceived privacy risks, suggesting that better privacy

practices would have aligned with both ethical requirements and business interests by increasing user trust and engagement.

VI. Defense Strategies

A. Technical Defenses

Effective technical defense strategies against unauthorized access to voice recordings combine both preventive and detective controls.

1) End-to-End Encryption and Data Minimization: Implementing robust encryption and data minimization practices represents the foundation of technical defense:

- **End-to-end encryption**: Ensuring voice data remains encrypted throughout its lifecycle
- **Voice data minimization**: Limiting what is recorded and transmitted to essential content only
- **Selective recording**: Only capturing the specific command, not preceding or following audio
- **Offline processing**: Expanding capabilities for processing commands without cloud transmission

Singh et al. [23] proposed device-originated TLS tunnels terminating in hardware security modules as a critical defense mechanism. Their research emphasized zero-trust access control with fine-grained OAuth scopes per device-service pair, coupled with automated key rotation to minimize unauthorized access risks.

2) Technical Architectures for Privacy: Several architectural approaches can enhance privacy protection:

- **Ephemeral storage**: Automatically deleting recordings after processing
- **Audio truncation**: Removing ambient sounds before and after commands
- **Speaker identification**: Verifying the speaker before processing sensitive commands
- **Secure communication channels**: Ensuring all device-cloud interactions use secure protocols

Edu et al. [19] identified presence-based controls using Wi-Fi or BLE beacons to ensure commands only execute when authorized users are nearby. While noting these could potentially be spoofed, their research suggested that layered defenses combining multiple technical approaches provided the most robust protection.

Bolton et al. [17] specifically recommended robust wake-word spoofing detection and granular consent UIs that precisely mapped which data was shared. Their architectural diagram highlighting the four risk zones in the voice assistant pipeline provides a framework for implementing targeted defenses at each vulnerable point.

Cheng and Roedig [18] categorized voice privacy threats as one of four main categories of personal voice assistant risks, alongside access control, acoustic denial-of-service, and acoustic sensing. Their comprehensive taxonomy emphasizes the need for multi-faceted defense approaches addressing each vulnerability class.

B. Policy and Procedural Defenses

Technical measures alone are insufficient; they must be complemented by robust policy and procedural defenses.

1) User Control and Consent Mechanisms: Enhancing user agency through improved control and consent:

- **Opt-in consent**: Requiring affirmative permission before any recording review
- **User data controls**: Providing accessible dashboards for managing voice data
- **Recording indicators**: Clear visual or audible signals when recording is active
- **Audio deletion policies**: Simple mechanisms for users to delete stored recordings

Vardakis et al. [24] emphasized the importance of user awareness, recommending step-by-step guides for secure configuration and automated firmware update reminders. Their research highlighted how technical safeguards must be accompanied by usable interfaces that empower users to implement available protections.

2) Transparency and Accountability Measures: Organizations must implement systematic transparency and accountability:

- **Transparent disclosures**: Clear communication about data practices in accessible language
- **Privacy dashboards**: Centralized interfaces showing what data is collected and how it's used
- **Third-party audits**: Independent verification of privacy practices
- **Data processing agreements**: Clear contractual limitations on how data can be used

Maccario and Naldi [22] called for interdisciplinary research linking technical, legal, and social perspectives on voice assistant privacy. Their systematic review highlighted the need for integrating these complementary approaches rather than treating them as separate domains.

Sharif and Tenbergen [20] identified six main vulnerability types in smart home voice assistants, recommending that vendors adopt two-factor voice authentication, sandboxed skill execution, and publish clear user guidance on device hardening. Their vulnerability taxonomy provides a framework for comprehensive procedural defenses addressing each risk category.

VII. Corporate Mitigation Measures

A. Immediate Response Actions

When privacy breaches involving voice recordings were publicly revealed, companies implemented several immediate mitigation measures.

1) Program Suspensions and Policy Updates: Initial corporate responses included:

- **Program suspension**: Temporarily halting human review programs
- **Policy updates**: Revising terms of service to explicitly acknowledge review practices
- **Customer notification**: Informing users about past practices and changes
- **Retroactive consent**: Seeking permission for existing data and future review

Maccario and Naldi [22] tracked the evolution of privacy research and corporate responses, noting that consumer awareness and vendor practices evolved significantly following public disclosures of review programs.

2) Crisis Management and User Trust: Companies also implemented measures to rebuild user trust:

- **Recording deletion**: Offering simplified ways to delete historical recordings
- **Public relations management**: Communicating changes and commitments
- **Crisis response**: Addressing media and regulatory inquiries
- **Compensation measures**: In some cases, offering credits or extended services

Tsourakas et al. [21] noted how privacy concerns led to under-use of voice assistant applications, highlighting the business imperative for effective crisis response to prevent user abandonment of services.

B. Long-term Strategic Changes

Beyond immediate responses, meaningful mitigation required fundamental strategic changes in how voice data is handled.

1) Privacy Culture and Governance: Sustainable changes required shifts in organizational culture:

- **Privacy culture**: Making privacy central to product development
- **Ethical AI development**: Integrating ethical considerations throughout the development lifecycle
- **Employee ethics training**: Ensuring all staff understand privacy responsibilities
- **Data governance**: Implementing systematic oversight of data handling

Cheng and Roedig [18] emphasized the need for comprehensive approaches to voice assistant privacy and security, noting that effective protection requires the integration of privacy considerations throughout product development rather than as an afterthought.

2) Systematic Privacy Protections: Long-term solutions involved implementing systematic protections:

- **Privacy impact assessments**: Evaluating privacy implications before launching features
- **Privacy champions**: Designating internal advocates for user privacy
- **Responsible innovation**: Balancing functionality with privacy protections
- **Trust rebuilding**: Demonstrating ongoing commitment to privacy through actions

Singh et al. [23] recommended standardizing lightweight attestation protocols for constrained devices and integrating user-facing privacy dashboards for transparent data flows. Their framework emphasizes that security and privacy must be built into systems from initial designs rather than added later.

Bolton et al. [17] and Edu et al. [19] both highlighted the need for robust and standardized vendor transparency reports, allowing users and regulators to verify adherence to privacy commitments through ongoing monitoring rather than relying solely on post-breach responses.

VIII. Consumer Protection Strategies

With the realization that voice recordings from smart speakers may be accessed by humans without explicit consent, consumers need practical strategies to protect their privacy while still benefiting from the convenience of voice assistants.

A. Settings and Controls

Smart speaker users can significantly reduce privacy risks through available device and account settings.

1) Physical Privacy Controls: The most immediate privacy protection comes from hardware controls built into devices:

- **Mute buttons**: All major smart speakers include physical microphone mute buttons that mechanically disconnect the microphone circuit, preventing any audio capture regardless of software status [17]. These physical switches provide stronger protection than software-based muting because they cannot be remotely circumvented.
- **Visual indicators**: Users should verify that devices properly display when microphones are active through LED indicators. However, Sharif and

Tenbergen [20] caution that these are sometimes too subtle or may be overlooked during regular use, suggesting the need for more prominent status indicators.

- **Positioning and placement**: Strategic positioning of devices away from private spaces (bedrooms, bathrooms) can limit exposure of sensitive conversations. Bolton et al. [17] note that consumers should consider sound propagation patterns within their homes when placing devices.

Lin et al. [25] demonstrated the feasibility of embedding privacy filters directly at the hardware level in their SR-PII system, which scans transcribed utterances for personally identifiable information before forwarding to cloud services. Their research shows that local privacy filtering can be implemented with negligible additional processing delay (maintaining 89-93% accuracy across different environmental conditions), suggesting future devices could include more sophisticated hardware-level protections.

2) Software Settings and Controls: Beyond physical controls, several software settings can enhance privacy:

- **Voice history deletion**: All major platforms offer options to delete historical recordings, though interfaces and retention periods vary. Users should regularly review and delete unwanted recordings through companion apps or web interfaces [18].
- **Activity controls**: Platforms typically allow customization of which activities are recorded and stored. Hyma et al. [10] recommend creating a personalized privacy profile that specifies exactly which types of interactions can be stored.
- **Account settings**: Users should review privacy settings in their linked accounts (Amazon, Google, Apple) to disable features like voice purchasing without verification, which might be triggered accidentally [20].
- **Recording review**: Some platforms now allow users to opt out of human review of recordings specifically while maintaining core functionality, a feature implemented after the privacy breach revelations [22].

Tabassum et al. [3] found that comfort with service and perceived usefulness positively correlate with willingness to share conversation data, suggesting that users make privacy decisions based on functionality trade-offs. Their research emphasizes the importance of clear controls that allow users to selectively enable features based on personal privacy preferences.

B. Alternative Products and Services

For users with heightened privacy concerns, several alternatives to mainstream voice assistants exist.

1) Privacy-Focused Voice Assistants: Several emerging options prioritize privacy by design:

- **Open-source voice assistants**: Solutions like Mycroft AI operate with transparent, auditable code and prioritize local processing when possible, reducing cloud dependency [19].
- **Local processing devices**: Systems that perform speech recognition and command execution locally, without transmitting voice data to cloud servers, eliminate the risk of remote access to recordings. Lin et al. [25] demonstrated the technical feasibility of such systems, achieving over 90% accuracy with privacy protection even in noisy environments.
- **Decentralized systems**: Some solutions use blockchain or federated approaches to distribute processing and reduce centralized data collection, though Hassan et al. [26] note that these may introduce new security considerations around distributed architecture.

2) Modified Usage Patterns: Users can adapt how they interact with existing devices:

- **Selective enabling**: Using the mute button by default and only unmuting when actively needing assistance reduces continuous listening risks [17].
- **Manual controls**: Integrating voice assistants with physical buttons or switches for critical functions (smart locks, security systems) provides backup control methods [24].
- **Disconnected smart home**: Implementing local hub-based smart home systems that operate independently of voice assistants allows for automation without voice data transmission [26].
- **Offline functionality**: Choosing devices with local command processing capabilities for basic functions enables core features without network connectivity, as demonstrated by Lin et al.'s [25] offline speech recognition system.

Hassan et al. [26] emphasize the importance of understanding the four-layer IoT architecture (Perception, Network, Middleware, Application) when selecting alternative solutions, as security vulnerabilities may exist at any layer. Their research suggests that privacy-focused alternatives should implement security features across all architectural layers to be truly effective.

IX. IoT Security Awareness and Education

Beyond individual protection measures, broader educational initiatives are essential to improve understanding of voice assistant privacy risks and safeguards.

A. Effective Communication Strategies

Communicating complex privacy concepts effectively requires specialized approaches.

1) Making Privacy Tangible: Abstract privacy risks need to be translated into understandable terms:

- **Privacy analogies**: Comparing voice recording review to having an unknown person listening to phone calls can help convey the privacy implications in relatable terms [21].
- **Risk communication frameworks**: Structured approaches to explaining probability and impact of privacy breaches help users make informed decisions. Bensalem et al. [27] advocate for "algorithmic notice" protocols that clearly communicate exactly which data points feed into smart device systems.
- **Visualization techniques**: Visual representations of data flows can illustrate what happens when voice commands are processed, making abstract concepts concrete [6].

Tsourakas et al. [21] found that many students underuse voice assistant applications due to perceived privacy risks, highlighting the importance of clear communication about both risks and protections to enable informed use.

2) Technology Transparency Approaches: Improving digital literacy requires demystifying the technology:

- **Plain language explanations**: Technical concepts should be explained without jargon, focusing on practical implications rather than technical details [28].
- **Privacy trade-offs clarification**: Honest communication about the functionality benefits and privacy costs of different features allows users to make value-aligned choices [3].
- **Informed decision-making tools**: Interactive guides that walk users through privacy settings with clear explanations of consequences support better choices [27].

Hamilton et al. [28] proposed a standardized agency rating system (similar to energy-efficiency labels) that would assess voice assistants on dimensions including data privacy, ethical design, transparency, social impact, and legal compliance. Such systems could significantly enhance consumer understanding of privacy implications when selecting and configuring devices.

B. Community and Family Education

Voice assistants impact not just individual users but entire households, requiring family-level approaches to privacy.

1) Household Management Strategies: Families need coordinated approaches to device management:

- **Family tech policies**: Establishing household guidelines for voice assistant use, including when devices should be muted or which commands are permitted [8].
- **Parental controls**: Implementing age-appropriate restrictions for child users to prevent unauthorized purchases or access to inappropriate content [21].
- **Shared device policies**: Creating agreements about who can access voice histories and what information is appropriate to share through communal devices [20].

Mckie et al. [8] observed that long-term users develop personified relationships with voice assistants (e.g., "Uncle Google," "Auntie Alexa"), which may influence privacy perceptions. Their research suggests that family discussions should address these personification tendencies when establishing privacy boundaries.

2) Generational Considerations: Different age groups have varying privacy concerns and technical abilities:

- **Age-appropriate explanations**: Tailoring privacy discussions to different age groups, from simplified concepts for children to detailed controls for adults [21].
- **Digital citizenship education**: Incorporating voice assistant privacy into broader digital literacy education about responsible technology use [29].
- **Tech boundaries**: Establishing clear expectations about device usage times and acceptable commands for children [21].

Demir et al. [29] investigated voice assistants in educational contexts, finding them to be efficient tools for answering research queries and solving math problems, but noting adoption barriers related to privacy concerns. Their research highlights the need for educational approaches that balance the benefits of voice technology with appropriate privacy protections, particularly when used by young people.

C. Advocacy and Information Sharing

Broader systemic change requires collective action and knowledge sharing.

1) Rights Awareness and Consumer Advocacy: Informing users about their legal protections:

- **Consumer rights education**: Teaching users about their legal entitlements regarding data collection and privacy under relevant regulations like GDPR, CCPA, and others [27].
- **Privacy advocacy organizations**: Connecting consumers with advocacy groups that provide resources, tools, and collective representation on voice assistant privacy issues [22].
- **Digital rights frameworks**: Understanding voice assistant privacy within broader digital rights contexts, including informed consent and data minimization principles [27].

Bensalem et al. [27] analyzed the relationship between AI, big data, and consumer privacy, highlighting regulatory gaps that require AI-specific guidelines within existing frameworks to address real-time decision-making and automated content generation. Their research emphasizes the need for cross-functional governance that unites technical, privacy, and legal expertise.

2) Community Resources and Engagement: Fostering community knowledge sharing:

- **Public awareness campaigns**: Supporting initiatives that educate consumers about privacy risks and protection strategies for voice assistants [22].
- **Community workshops**: Organizing local events where users can learn practical privacy skills and device configuration techniques [21].
- **Online resources**: Creating and sharing comprehensive guides, tutorials, and verification tools for privacy-enhancing configurations [26].
- **Policy engagement**: Participating in public comments, legislative hearings, and other opportunities to shape voice assistant privacy regulations [27].

Maccario and Naldi [22] traced the evolution of privacy research on smart speakers, showing how publications grew at a 63.45% compound annual rate from 2017 through 2021. Their systematic review demonstrates the rapid expansion of knowledge in this area and the need for translating this research into accessible community resources.

X. Future Directions

The landscape of voice assistant privacy is rapidly evolving, with technological innovations, regulatory developments, and changing user expectations shaping future trends.

A. Emerging Privacy Technologies

Technological solutions for voice assistant privacy are advancing rapidly, with several promising approaches on the horizon.

1) Real-time Privacy Enforcement: Next-generation privacy protection will rely on automated, real-time enforcement:

- **Privacy compliance firewalls**: Ahmad et al. [30] developed Eunomia, a ground-breaking real-time privacy firewall for Alexa skills that intercepts and validates interactions against published privacy policies. Their system demonstrated 96-100% precision in detecting policy violations and identified approximately 1,405 skills (2.5%) requesting sensitive data without corresponding policy disclosures. This approach marks a shift from retrospective analysis to preventative protection.
- **Privacy identification systems**: Building on Lin et al.'s [25] work on privacy identification for social robots, more sophisticated systems could automatically filter sensitive information at the edge before it reaches cloud services, with negligible impact on performance.
- **Unified privacy dashboards**: Hernández Acosta and Reinhardt [31] found strong consensus ($\geq$80%) among smart speaker users for comprehensive privacy dashboards summarizing data flows and offering one-click revocation of third-party access. Their research revealed significant brand differences in privacy preferences, with Amazon users showing the highest trust in default data practices, while Google and Apple users demonstrated greater desire for manual data deletion controls.

2) Domain-Specific Applications: Privacy-preserving voice assistants are being adapted for specialized contexts:

- **Industrial and collaborative environments**: Arntz [32] demonstrated how voice assistants can enhance human-robot collaboration in virtual reality environments, enabling natural dialogue for industrial applications. This work highlights the need for privacy-conscious approaches as voice technology extends into workplace settings.
- **Accessibility applications**: Jakob et al. [33] conducted a longitudinal study of voice assistant adoption among adults aged 55+, finding that privacy

concerns decreased from 60% to 25% over a 12-week period as users became comfortable with the technology. Their work emphasizes the importance of multimodal feedback and accessible tutorials to enhance user confidence and privacy awareness.
- **Healthcare integration**: Voice assistants are increasingly being adapted for healthcare applications, raising new privacy considerations under regulatory frameworks like HIPAA. Building on Sharon's [34] analysis of technology companies' role in health policy, future voice assistants will require specialized privacy frameworks for sensitive health data.

B. Regulatory and Policy Evolution

The regulatory landscape governing voice assistant privacy is likely to see significant development.

1) Standardized Privacy Requirements: Evolving regulations may establish consistent standards:

- **Mandatory transparency**: Future regulations might require standardized disclosures about when recordings are transmitted, stored, and accessed by humans, addressing the transparency gaps that enabled the privacy breach [31].
- **Design mandates**: As Hartzog et al. [35] argue, small privacy "nicks" that are minor but frequent privacy intrusions ignored by law, cumulatively normalize expansive surveillance. Their work suggests that design mandates requiring privacy-preserving defaults and transparency will become increasingly important in regulating voice technologies.
- **Cross-jurisdictional frameworks**: International coordination on privacy standards could prevent regulatory fragmentation, allowing consistent user experiences across regions.

2) Corporate Governance and Accountability: New accountability frameworks are emerging:

- **Third-party certification**: Independent privacy audits and certification programs could provide users with trustworthy information about voice assistant privacy practices [31].
- **Algorithmic impact assessments**: Similar to environmental impact assessments, these evaluations would document the privacy implications of voice processing systems before deployment.
- **Sphere encroachment protection**: Sharon [34] cautions against technology companies' undue influence in policy spheres beyond their core expertise, suggesting that future governance frameworks must balance innovation with democratic accountability and prevent corporate overreach.

C. Evolving User Expectations

User attitudes and behaviors toward voice assistant privacy are changing over time.

1) Privacy Literacy and Awareness: As users become more sophisticated about privacy:

- **Generational shifts**: Younger users with lifelong technology exposure may have different privacy expectations than older generations, though Jakob et al. [33] found that even older adults can develop comfort with voice assistants through extended use.
- **Privacy differentiation**: Users increasingly distinguish between different types of data, with varying sensitivity levels assigned to different interactions [31].
- **Control granularity**: Hernández Acosta and Reinhardt [31] found that 65% of users wanted finer-grained permission controls for individual third-party "skills," indicating growing sophistication in privacy preferences.

2) Trust Restoration and Verification: Rebuilding trust after privacy breaches requires new approaches:

- **Verification over trust**: Moving from trust-based to verification-based privacy models where users can independently confirm how their data is handled [30].
- **Continuous consent**: Dynamic, context-sensitive permission systems that adapt to changing user preferences and interaction contexts.
- **Visual privacy indicators**: Hernández Acosta and Reinhardt [31] found that over 70% of users wanted real-time visual indicators (e.g., LED codes) of active listening, demonstrating demand for immediate feedback about device status.

The evolution of voice assistant privacy will require ongoing collaboration between technology developers, policymakers, privacy advocates, and users to establish norms and standards that protect privacy while enabling beneficial voice interactions.

XI. Conclusion

This research has examined the significant privacy breach involving employee access to voice recordings from smart speakers produced by Amazon, Google, and Apple, analyzing its causes, impacts, and implications for privacy protection in voice-enabled technologies.

The investigation has revealed several critical insights about the nature and scope of the privacy breach:

First, the privacy incident stemmed from a fundamental disconnect between user expectations and actual practices. Users reasonably assumed their voice interactions remained private or were processed only by automated systems, but in reality, thousands of human reviewers systematically accessed recordings, including accidentally captured conversations, for quality assurance purposes. This gap represents a significant failure in transparency and informed consent.

Second, the technical architecture of voice assistants created inherent privacy vulnerabilities. The combination of wake word detection limitations, cloud-based processing, and quality assurance requirements created multiple points where privacy could be compromised. False activations triggered by ambient sounds or misinterpreted phrases resulted in the unintentional recording and human review of private conversations.

Third, the impact extended beyond individual privacy concerns to raise broader questions about power dynamics in digital ecosystems. As Hartzog et al. [35] argue, small privacy "nicks", like the normalization of ambient listening, cumulatively normalize expansive surveillance and create a "disempowerment spiral" where users gradually accept increasingly intrusive practices.

Fourth, effective privacy protection requires a multi-layered approach combining technical safeguards, procedural controls, regulatory frameworks, and user education. No single solution can fully address the complex privacy challenges inherent in voice assistant systems.

A. Broader Implications

The smart speaker privacy breach has implications that extend far beyond these specific incidents:

The case illustrates the privacy challenges that arise when consumer technologies deploy always-on sensors in intimate spaces. As Sharon [34] argues in the context of health applications, when technology companies expand into new domains, they can exercise undue influence through technological advantage, raising concerns about "sphere encroachments" into personal and private realms.

The findings also demonstrate how convenience and functionality can overshadow privacy concerns in consumer decision-making. Hernández Acosta and Reinhardt [31] found that despite awareness of privacy issues, only approximately 45% of users regularly review or delete their voice recordings as per Table I, with perceived complexity and lack of notification about existing settings serving as primary barriers.

Voice Recordings and Transcripts about	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)
Personal prefs	5	6	12	30	47
Financial issues	4	5	11	28	52
False actions	5	5	10	28	52
Guests	6	6	14	30	44
Children	6	6	14	30	44

TABLE I: Percentage distribution of participant responses (Strongly disagree → Strongly agree) to the prompt "I would tend to delete…" for five categories of voice recordings and transcripts: personal preferences, financial issues, false activations, guests, and children. [31]

The research highlights the need for privacy-by-design approaches that embed protection into technology from inception rather than as an afterthought. Ahmad et al.'s [30] Eunomia system demonstrates the feasibility of real-time privacy enforcement that can prevent violations before they occur rather than addressing them retroactively.

Finally, the case underscores the importance of demographic considerations in privacy protection. Jakob et al. [33] found that privacy concerns among older adults decreased substantially over extended use periods, suggesting that privacy approaches must account for varying levels of technology familiarity and adapt to changing perceptions over time.

B. The Path Forward

Moving forward, several principles should guide the evolution of voice assistant privacy:

Transparency and control must be foundational elements of voice assistant systems. Users deserve clear information about how their voice data is processed and meaningful control over who can access their recordings. Hernández Acosta and Reinhardt [31] found strong user demand for unified privacy dashboards and visual indicators of active listening, suggesting specific implementation paths for enhancing transparency.

Technical innovation should prioritize privacy-preserving approaches like on-device processing, improved wake word accuracy, and real-time privacy filtering. Lin et al. [25] demonstrated that embedding privacy filters directly at the hardware level can maintain high accuracy while protecting sensitive information.

Regulatory frameworks need to evolve beyond addressing large privacy "chops" to also recognize the cumulative impact of privacy "nicks" that normalize surveillance, as articulated by Hartzog et al. [35]. This may require collective rights frameworks, design mandates, and outright bans on particularly pernicious practices.

Educational initiatives should help users understand both the benefits and risks of voice technologies, enabling informed decisions about adoption and configuration. As voice assistants expand into new domains like industrial collaboration [32] and healthcare [34], targeted education for these specialized contexts will become increasingly important.

In conclusion, the smart speaker privacy breach involving employee access to voice recordings represents not just a technical or procedural failure, but a fundamental challenge to how we conceptualize privacy in an increasingly voice-activated world. By implementing comprehensive technical safeguards, strengthening regulatory oversight, enhancing user control, and improving privacy education, we can work toward voice assistant ecosystems that respect user privacy while delivering the convenience and functionality that make these technologies valuable. The critical task ahead is not choosing between innovation and privacy, but rather developing approaches that thoughtfully integrate both.

References

[1] V. Morozovaite, "The future of anticompetitive self-preferencing: analysis of hypernudging by voice assistants under article 102 tfeu," *European Competition Journal*, vol. 19, pp. 410–448, 04 2023.

[2] S. Anayat, G. Rasool, and A. Pathania, "Examining the context-specific reasons and adoption of artificial intelligence-based voice assistants: A behavioural reasoning theory approach," *International Journal of Consumer Studies*, vol. 47, pp. 1885–1910, 06 2023.

[3] M. Tabassum, T. Kosiński, A. Frik, N. Malkin, P. Wijesekera, S. Egelman, and H. R. Lipford, "Investigating users' preferences and expectations for always-listening voice assistants," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, pp. 1–23, 12 2019.

[4] D. Buhalis and I. Moldavska, "Voice assistants in hospitality: using artificial intelligence for customer service," *Journal of Hospitality and Tourism Technology*, vol. 13, pp. 386–403, 12 2021.

[5] D. Commisso, "Has the smart speaker market peaked?" CivicScience, 12 2021. [Online]. Available: https://civicscience.com/has-the-smart-speaker-market-peaked/

[6] B. Minder, P. Wolf, M. Baldauf, and S. Verma, "Voice assistants in private households: a conceptual framework for future research in an interdisciplinary field," *Humanities and Social Sciences Communications*, vol. 10, 04 2023.

[7] D. S. Zwakman, D. Pal, and C. Arpnikanondt, "Usability evaluation of artificial intelligence-based voice assistants: The case of amazon alexa," *SN Computer Science*, vol. 2, 01 2021.

[8] I. Mckie, B. Narayan, and B. Kocaballi, "Conversational voice assistants and a case study of long-term users: A human information behaviours perspective," *Journal of the Australian Library and Information Association*, vol. 71, pp. 233–255, 07 2022.

[9] G. Maccario and M. Naldi, "Alexa, is my data safe? the (ir)relevance of privacy in smart speakers reviews," *International Journal of Human–Computer Interaction*, vol. 39, pp. 1244–1256, 04 2022.

[10] J. Hyma, M. R. K. Murty, and A. Naveen, "Personalized privacy assistant for digital voice assistants: Case study on amazon alexa," *International Journal of Knowledge-based and Intelligent Engineering Systems*, vol. 25, pp. 291–297, 11 2021.

[11] B. R. Barricelli, A. Bondioli, D. Fogli, L. Iemmolo, and A. Locoro, "Creating routines for iot ecosystems through conversation with smart speakers," *International Journal of Human–Computer Interaction*, vol. 40, pp. 6109–6127, 08 2023.

[12] M. Alzate, M. Arce Urriza, and M. Cortiñas, "Voice-activated personal assistants and privacy concerns: a twitter analysis," *Journal of Research in Interactive Marketing*, vol. 18, pp. 611–630, 11 2023.

[13] D. Mavrova Heinrich and J. Cook, "Ai-ready attorneys: Ethical obligations and privacy considerations in the age of artificial intelligence," *SSRN Electronic Journal*, 2024.

[14] T. Lyu, Y. Guo, and H. Chen, "Understanding the privacy protection disengagement behaviour of contactless digital service users: the roles of privacy fatigue and privacy literacy," *Behaviour amp; Information Technology*, vol. 43, pp. 2007–2023, 07 2023.

[15] V. Pitardi and H. R. Marriott, "Alexa, ¡i¿she's¡/i¿ not human but… unveiling the drivers of consumers' trust in voice-based artificial intelligence," *Psychology amp; Marketing*, vol. 38, pp. 626–642, 01 2021.

[16] S. Molinillo, F. Rejón-Guardia, R. Anaya-Sánchez, and F. Liébana-Cabanillas, "Impact of perceived value on intention to use voice assistants: The moderating effects of personal innovativeness and experience," *Psychology amp; Marketing*, vol. 40, pp. 2272–2290, 09 2023.

[17] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and A. H. Sodhro, "On the security and privacy challenges of virtual assistants," *Sensors*, vol. 21, p. 2312, 03 2021.

[18] P. Cheng and U. Roedig, "Personal voice assistant security and privacy—a survey," *Proceedings of the IEEE*, vol. 110, pp. 476–507, 04 2022.

[19] J. S. Edu, J. M. Such, and G. Suarez-Tangil, "Smart home personal assistants," *ACM Computing Surveys*, vol. 53, pp. 1–36, 12 2020.

[20] K. Sharif and B. Tenbergen, "Smart home voice assistants: A literature survey of user privacy and security vulnerabilities," *Complex Systems Informatics and Modeling Quarterly*, pp. 15–30, 10 2020.

[21] T. Tsourakas, G. Terzopoulos, and S. Goumas, "Educational use of voice assistants and smart speakers," *Journal of Engineering Science and Technology Review*, vol. 14, pp. 1–9, 2021.

[22] G. Maccario and M. Naldi, "Privacy in smart speakers: A systematic literature review," *SECURITY AND PRIVACY*, vol. 6, 10 2022.

[23] N. Singh, R. Buyya, and H. Kim, "Securing cloud-based internet of things: Challenges and mitigations," *Sensors*, vol. 25, p. 79, 12 2024.

[24] G. Vardakis, G. Hatzivasilis, E. Koutsaki, and N. Papadakis, "Review of smart-home security using the internet of things," *Electronics*, vol. 13, p. 3343, 08 2024.

[25] P.-C. Lin, B. Yankson, V. Chauhan, and M. Tsukada, "Building a speech recognition system with privacy identification information based on google voice for social robots," *The Journal of Supercomputing*, vol. 78, pp. 15 060–15 088, 04 2022.

[26] A. Hassan, N. Nizam-Uddin, A. Quddus, S. R. Hassan, A. U. Rehman, and S. Bharany, "Navigating iot security: Insights into architecture, key security features, attacks, current challenges and ai-driven solutions shaping the future of connectivity," *Computers, Materials amp; Continua*, vol. 81, pp. 3499–3559, 2024.

[27] A. Merrakchi, "Symbiosis or surveillance? exploring the relationship between ai, big data, and consumer privacy in digital marketing symbiosis or surveillance? exploring the relationship between," 07 2024.

[28] C. Hamilton, S. Korea, W. Swart, and G. Stokes, "Developing a measure of social, ethical, and legal content for intelligent cognitive assistants," *Journal of Strategic Innovation and Sustainability*, vol. 16, p. 2021.

[29] F. Demir, Research, and E. Jung, "Hey google, help doing my homework: Surveying voice interactive systems," *Journal of User Experience*, vol. 18, pp. 41–61, 2022.

[30] J. Ahmad, F. Li, R. Beuran, and B. Luo, "Eunomia: A real-time privacy compliance firewall for alexa skills," *2024 Annual Computer Security Applications Conference (ACSAC)*, pp. 650–665, 12 2024.

[31] L. Hernández Acosta and D. Reinhardt, ""alexa, how do you protect my privacy?" a quantitative study of user preferences and requirements about smart speaker privacy settings," *Computers amp; Security*, vol. 151, p. 104302, 04 2025.

[32] A. Arntz, "Enhancing human-robot collaboration in virtual reality: A task-driven communication system using alexa voice service," 2025.

[33] D. Jakob, S. Wilhelm, A. Gerl, D. Ahrens, and F. Wahl, "Adapting voice assistant technology for older adults: A comprehensive study on usability, learning patterns, and acceptance," *Digital*, vol. 5, p. 4, 01 2025.

[34] T. Sharon, "Blind-sided by privacy? digital contact tracing, the apple/google api and big tech's newfound role as global health policy makers," *Ethics and Information Technology*, vol. 23, pp. 45–57, 07 2020.

[35] W. Hartzog, E. Selinger, and J. Gunawan, "Privacy nicks: How the law normalizes surveillance," *SSRN Electronic Journal*, 2023.