UNINTENDED LISTENERS: A CRITICAL ANALYSIS OF AMBIENT VOICE RECORDINGS UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Saanvi Aggarwal, School of Law, CHRIST (Deemed to be University), Bangalore

ABSTRACT

This paper examines voice-activated assistants such as smart speakers and phone-based voice agents, for example, Amazon Alexa, Google Assistant, and Apple Siri, with particular focus on their impact on users' privacy under India's Digital Personal Data Protection (DPDP) Act, 2023. While these devices are marketed as being activated only by clear "wake words", the researcher uses global evidences to show that they often trigger accidentally and capture sensitive background conversations without the knowledge of users. The paper adopts a doctrinal approach and critically analyses the DPDP Act to assess how well it addresses or fails to address such issues. The scope of this paper is limited to the Indian context of the DPDP Act, 2023, and does not provide an exhaustive study of privacy laws in other jurisdictions. Further, the focus is restricted to smart speakers and phone-based voice assistants, excluding other forms of Internet of Things (IoT) devices. The key finding of this paper is that the DPDP Act introduces principles of consent and purpose limitation, yet it neglects continuous ambient recordings and accidental recordings. The lack of explicit rules for such situations weakens user control and fails to adequately protect personal information, allowing Data Fiduciaries to potentially retain and misuse sensitive conversations. To fill this gap, the paper proposes reforms such as introducing a clear definition of "ambient data", requiring explicit consent for its collection, mandating on-device processing by default, and enforcing strict deletion protocols for mis-triggered recordings. The paper also suggests greater responsibility on companies to disclose how often such mis-triggered activations happen, and to undergo independent audits to enhance wake-word listening and data management by voice assistants. In conclusion, although the DPDP Act shows progress, the existing gaps pose a threat to digital dignity and the fundamental right to privacy as under Article 21 of the Constitution.

Keywords: Voice assistant surveillance, Ambient recording, Accidental activation, Digital Personal Data Protection Act (DPDP Act), Right to Privacy

I. INTRODUCTION

Voice assistants such as Amazon Alexa, Apple Siri, and Google Assistant are often present in modern homes. These are applications that are designed to respond to voice commands and perform various tasks. Voice Assistants provide ease, like delivering quick notifications, prompt replies, and even controlling home elements, such as lighting or grocery orders, all through voice commands. Nonetheless, this ease brings a cost. For functioning, these assistants depend on a "wake word", which is a particular phrase like "Alexa" or "Hey Siri" that gives signals to the device to start recording. To capture the wake word, the microphone of the device is always active[1]. This "always–active" design means that background conversations are being continuously recorded, even when the users did not intend to turn the device on.

Real-life instances show time and again how the threat of ambient sound recordings has turned real. For example, in 2017, a Super Bowl commercial by Google unintentionally activated Google Home devices and Google Phone Assistants across the United States upon hearing the phrase, 'Okay, Google'[2]. In 2018, The Guardian reported how Alexa had recorded a private discussion by mistake and forwarded these recordings to a contact[3]. In the same year, Forbes raised concerns about whether Voice Assistants like Alexa and Google Assistant eavesdrop and record private conversations beyond commands using wake words[4]. These cases are still on the rise, as more recently, it was reported that Siri had accidentally recorded conversations without people's consent. In February 2025, Apple reached a $95 million settlement in a consolidated class-action lawsuit regarding allegations that Siri recorded conversations without users' permission. The lawsuits claimed that Siri was occasionally activated by background noises rather than its wake word, leading to audio recordings being stored and, in certain instances, analyzed by contractors for performance enhancement. The plaintiffs contended that this action infringed upon privacy rights and consumer protection regulations, as users were not sufficiently informed or provided with a choice[5].

---

[1] A. HERNÁNDEZ ACOSTA & D. REINHARDT, *A Survey on Privacy Issues and Solutions for Voice-controlled Digital Assistants*, 80 PERVASIVE & MOBILE COMPUTING 1, 3–4 (2022).

[2] *Google Super Bowl Ad Inadvertently Triggers Voice-Activated Google Home Speakers*, THE DRUM (Feb. 6, 2017), https://www.thedrum.com/news/2017/02/06/google-super-bowl-ad-inadvertently-triggers-voice-activated-google-home-speakers.

[3] Samuel Gibbs, *Amazon Alexa Recorded Private Conversation and Sent It to Random Contact*, THE GUARDIAN (May 24, 2018), https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation.

[4] Blake Morgan, *Are Digital Assistants Always Listening?*, FORBES (Feb. 5, 2018), https://www.forbes.com/sites/blakemorgan/2018/02/05/are-digital-assistants-always-listening.

[5] *Apple's $95 Million Siri Settlement Explained: Who Qualifies, How Much You'll Get, and How to Claim*, THE

These concerns have extended beyond the West, and even the Indian media has started to question whether Alexa, Google, and Siri invade privacy by capturing ambient audio through accidental activations[6]. Researchers have linked these failures to issues in technical design. Wake-word detection can experience false positives, meaning that ordinary conversations or ambient sounds can be falsely recognized as a wake word[7]. Once the recording starts, data is transmitted to external remote servers, where it could be stored, analysed, or reviewed by human agents[8]. Research shows that such audio data often contains private information regarding the health, finances, and personal relationships of users, which is difficult to anonymize[9]. This is very risky if the data is misused. Shoshana Zuboff frames this within the broader framework of "surveillance capitalism," where businesses transform such information into commodities and engage in selling and buying under the guise of aiding innovation[10].

These advancements in technology are faster than the laws can keep up with. The European Union's General Data Protection Regulation (GDPR) requires consent to be clear and freely given[11]. Yet, scholars argue that the reality of constant ambient listening makes giving such clear consent impossible[12]. In California, the Consumer Privacy Act (CCPA) offers rights to know, delete, and opt out to users; however, critics claim these protections are insufficient, and their enforcement remains weak when people are unaware that unintentional ambient recordings happen[13]. Comparative research across Europe, North America, and Asia supports the researcher's observation that laws aimed at deliberate, conscious data sharing frequently fail when it comes to hidden and passive ambient sound recording[14].

ECONOMIC TIMES (Feb. 6, 2025), https://m.economictimes.com/news/international/global-trends/apples-95-million-siri-settlement-explained-who-qualifies-how-much-youll-get-and-how-to-claim/articleshow/121177203.cms.

[6] *Do Alexa, Google and Siri Really Listen to Our Conversation?*, TIMES OF INDIA (Mar. 6, 2024), https://timesofindia.indiatimes.com/etimes/trending/do-alexa-google-and-siri-really-listen-to-our-conversation/articleshow/114431914.cms

[7] TOM BOLTON ET AL., *On the Security and Privacy Challenges of Virtual Assistants*, 21 SENSORS 1, 4–6 (2021).

[8] W. ALBAYAYDH & I. FLECHAIS, *Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes*, *in* 33D USENIX SECURITY SYMPOSIUM 1, 2–3 (2024).

[9] PEPRAH OWUSU ET AL., *Privacy, Confidentiality and Ethical Concerns in Audio AI Assistants: A Comparative Study of North American, European, and Asian Markets*, 13(1) INT'L J. SCI. & RSCH. ARCHIVE 3023, 3026–27 (2024).

[10] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 201–04 (PublicAffairs 2019).

[11] Regulation (EU) 2016/679, art. 6, 2016 O.J. (L 119) 1.

[12] S. DE CONCA, *A Full House: Applying the GDPR to Vocal Assistants*, *in* BILETA CONF. PAPERS 1, 5–7 (2021).

[13] SHAILENDRA K. SHANDILYA ET AL., NAVIGATING THE REGULATORY LANDSCAPE IN AI AND SAFEGUARDING DATA PRIVACY 47–48 (2024).

[14] Owusu et al., *supra* note 9, at 3028–29.

India's legal framework reflects this worldwide conflict, but it also brings in unique constitutional implications. In K.S. Puttaswamy v. Union of India[15], the Supreme Court recognized privacy as a fundamental right under Article 21, directly associating it with dignity and autonomy. Justice Chandrachud's opinion emphasized that privacy is not granted by the Constitution but recognized by it. Justice Kaul went further, warning that modern technology makes it possible to "enter a citizen's house without knocking at his/her door."[16] This reasoning directly applies to voice assistants, which literally "enter" the private home through their always-on microphones.

The Digital Personal Data Protection Act, 2023 (DPDP Act), expands on this framework by laying down guidelines for consent, lawful processing, and fiduciary duties[17]. Section 6 requires that consent must be free and informed, Section 7 specifies purpose limitation, and Section 8 imposes general obligations on Data Fiduciaries. However, the law does not explicitly recognize "ambient data", which refers to recordings made without the user's intention to trigger the wake word. Scholars argue that such a gap in the law places users at risk, as companies might exploit vague consent agreements to justify the retention and analysis of unintended recordings even after their purpose is served[18]. Thus, this paper analyses these loopholes by asking whether Section 6 meaningfully protects users against unintended ambient recordings, whether Section 7 restricts processing in a way that covers these cases, and whether Section 8's fiduciary duties are enforceable enough to matter. By critically analysing these provisions in light of global practice and technical realities, the paper identifies loopholes that allow companies to overstep. The researcher also proposes reforms, including a statutory definition of "ambient data," on-device processing by default, and mandatory independent audits to check wake-word accuracy.

II. HISTORY AND JURISPRUDENTIAL ANALYSIS OF VOICE ASSISTANTS

Voice assistants are one of the most used technologies in the past decade, which has completely revolutionised the way we interact with devices. Apple first introduced Siri in 2011, which

[15] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[16] *Id.* at 113.
[17] Digital Personal Data Protection Act, No. 22 of 2023, §§ 6–8 (India).
[18] SUCHITRA SHEORAN, *Voice Assistants and Data Security: Navigating Ethical and Legal Concerns*, WHITE BLACK LEGAL: THE L.J. 23, 23–24 (2025).

allowed people to use voice commands with their iPhones instead of typing[19]. This was a groundbreaking innovation that started the rise of voice assistants in gadgets. Soon, Amazon built its Alexa in 2014 and integrated it with their Echo smart speakers, which could perform tasks such as playing music, handling calendars, and controlling other smart gadgets inside the house, with the user's voice[20]. Even Google launched its Google Assistant in 2016, which could be connected across devices[21].

All of these assistants work in the same manner, where they are always listening for a wake word like "Hey Siri", "Ok Google", or "Alexa" to ensure that they activate when such wake words are triggered[22]. This makes these always-listening devices risky in private spheres such as homes, as they can accidentally pick up other conversations without the user's intent. Reports have shown that private conversations, including critical subjects such as health details, family matters, etc, have been recorded without the knowledge of the user[23]. This shows how helpful voice assistants are, increasingly becoming a concern about privacy in private spheres of life, and making private data available to companies even without user consent.

These risks are significant. In legal theory, Natural Law philosophers such as John Locke contended that autonomy and human dignity are inherent rights[24]. Thus, the researcher contends that privacy should not be overlooked or taken away simply because an individual clicks "agree" on a complex document of terms and conditions. Thus, when voice assistants capture conversations without explicit consent, they infringe on these natural rights.

Philosopher John Stuart Mill, belonging to a Liberal school of thought, wanted to preserve liberty in the private sphere, where individuals could act freely without interference[25]. When devices perpetually listen, they encroach upon this personal space. This impacts the lives of individuals, both users and bystanders, and their liberty is restricted in their private sphere due to constant surveillance, even if no physical harm is caused. Autonomy here does not simply

[19] Brian Chen, *Apple's Siri Is a Truly Revolutionary Innovation*, HARV. BUS. REV. (Oct. 2011), https://hbr.org/2011/10/apples-siri-is-as-revolutionar.
[20] *Amazon Alexa*, ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/technology/Amazon-Alexa (last visited Sept. 5, 2025).
[21] *Explore: Meet Google Assistant*, GOOGLE (May 2016), https://blog.google/intl/en-mena/product-updates/explore-get-answers/2016-google-assistant-en/.
[22] *Siri*, ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/technology/Siri (last visited Sept. 5, 2025).
[23] *Id.*
[24] JOHN LOCKE, *SECOND TREATISE OF GOVERNMENT* §§ 4–6 (C.B. Macpherson ed., Hackett Publ'g Co. 1980) (1690).
[25] JOHN STUART MILL, *ON LIBERTY* 14–17 (Elizabeth Rapaport ed., Hackett Publ'g Co. 1978) (1859).

mean the absence of state coercion, but also includes the ability to live freely without corporate monitoring.

Roscoe Pound, belonging to the sociological school of jurisprudence, views law as social engineering and emphasises the need for laws to adapt to societal demands[26]. Voice assistants influence behaviour in many ways, such as altering communication in a family, impacting household management, as well as affecting children's interactions with technology. Thus, the law should weigh these advantages against the risks of surveillance and modify itself to adapt to the realities of digital life.

The philosophy of Immanuel Kant intensifies the criticism. Kant had emphasised that humans must never simply serve as means to an end but rather as ends in themselves[27]. Modern models of consent tend to be long and obscure, as well as take advantage of the limited understanding of the user and leave the bystander, such as a child or guest, without any means of consent whatsoever. It minimises human beings to a data mining object, which compromises both the law and morality.

Lastly, the postmodern explanation of surveillance by Michel Foucault depicts the psychological impacts. His discussion of the Panopticon revealed that visibility, when continuous, makes people self-censor and behave differently[28]. Thus, even the threat of the possibility of the device listening will alter the way people behave, even in their most personal spheres.

Collectively, these histories and theories indicate that the issue of unintended recordings is not just a technical glitch. It is a conflict between technological convenience and the jurisprudential obligations to dignity, autonomy, and privacy. This premise explains why the regulatory instruments, such as the DPDP Act in India, should shift away from abstract principles of consent to deal with the practical implications of ambient surveillance.

III. REVIEW OF LITERATURE AND GAP IN EXISTING RESEARCH

The fast development of voice assistants has attracted the wide interest of the academic

[26] ROSCOE POUND, *JURISPRUDENCE* 338–40 (West Publ'g Co. 1959).
[27] IMMANUEL KANT, *THE METAPHYSICS OF MORALS* 42–45 (Mary Gregor trans., Cambridge Univ. Press 1996) (1797).
[28] MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* 200–05 (Alan Sheridan trans., Pantheon Books 1977).

community in computer science, law, and human-computer interaction. Existing literature, however, is useful, but it has failed to sufficiently align technical discoveries with statutory requirements in the Digital Personal Data Protection Act, 2023 (DPDP Act)[29] in India. In this section, I will review five representative studies, as regards what they add to what my paper attempts to fill the gaps.

1. Alexa, Can I Trust You? - Chung, Iorga, Voas & Lee (2017)[30]

This article by Chung and colleagues conducts an experiment that examined millions of network packets and proved that voice assistants sent recordings in plaintext to the servers that could be intercepted. They suggested a four-part taxonomy of threats, which includes covert eavesdropping, command hijacking, data exfiltration, and malicious skill injection. Software updates seal such flaws according to manufacturers; the authors demonstrated that vulnerabilities remain after every release of the firmware. This piece of work is invaluable in that it records how unintended recordings are technologically feasible and have continued to be exploited. Nevertheless, the article is very technical and does not address the question of how common users can be informed or guarded. To fill this gap, my paper will translate their forensic results into legally binding protections under the DPDP Act 6-8 and suggest the use of compulsory real-time notifications and ambient audio opt-in consent.

2. More Than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants - Abdi, Ramokapane & Such (2019)[31]

Abdi and colleagues, in the Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS), conducted interviews on how users perceive smart speakers, and came to the conclusion that many users think that muting a microphone stops recording, when in reality, the data was being stored in cloud servers. Their work shows the distorted perceptions users have and their lack of awareness of surveillance taking place. Their qualitative study is compelling but does not have a large and tech-savvy sample, which restricts the ability to generalise. Moreover, they suggest design enhancements, icons, and alerts, yet they do not relate these suggestions to binding legal rights. The researcher bases their analysis on this by

[29] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[30] JUDY CHUNG, ET AL., Alexa, Can I Trust You?, 50(9) *COMPUTER* 110, 112–14 (2017).
[31] NOURA ABDI ET AL., *More Than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants*, *in* PROCEEDINGS OF THE 15TH USENIX SYMPOSIUM ON USABLE PRIVACY & SECURITY 93, 97–99 (2019).

contextualising their findings in Section 7 of the DPDP Act, which governs processing. The paper suggests that there should be legal requirements of continuous transparency, like icons or sound alerts, to make sure that consent is informed, as indicated in Section 6.

3. **Eliciting Privacy Concerns for Smart Home Devices from a User-Centered Perspective - Chhetri & Motti (2019)[32]**

The article analysed 128 verified consumer reviews on smart home devices and found that privacy concerns were prevalent, and most consumers feared that their products were listening to them at all times. They grouped concerns into confidentiality, integrity, and availability, which proved that the anxieties of users are not peripheral or unsubstantiated. Their study has strength in being able to have the voices of the authentic users at scale. They are, however, descriptive as they raise issues, but never test interventions or legal consequences. This paper addresses this by relating the consumer distrust to statutory duties of Section 8 of the DPDP Act to argue that Data Fiduciaries should actively disclose mis-trigger rates and provide opt-out options to restore user trust.

4. **Security and Privacy Problems in Voice Assistant Applications: A Survey - Li, Chen, Pan & Others (2023)[33]**

An extensive survey was conducted by the authors that reviewed more than sixty papers on voice assistant vulnerabilities and reported that 40 percent of reported privacy breaches were due to unintentional wake-word triggering and that most of the technical defences have been tested only in laboratories. Their taxonomy of attack vectors, adversarial audio, replay attacks, and malicious skills offers a strict base for how threats should be understood. Their paper's scope, however, is limited to technical defences without having to refer to the user rights or regulatory responsibilities. This paper fills this gap by suggesting that Sections 16 (Privacy by Design) and 17 (Audits) of the DPDP Act explicitly require detection algorithms and independent audits to ensure that unintended recordings are disclosed and deleted.

5. **Voice Assistants and Data Security: Navigating Ethical and Legal Concerns -**

[32] CHOLA CHHETRI & VIVIAN GENARO MOTTI, *Eliciting Privacy Concerns for Smart Home Devices from a User-Centered Perspective*, *in* 11420 LECTURE NOTES IN COMPUTER SCIENCE 243, 248–50 (2019).
[33] JINGJIN LI ET AL., *Security and Privacy Problems in Voice Assistant Applications: A Survey*, arXiv:2301.01234, at 9–12 (2023), https://arxiv.org/abs/2301.01234.

Sheoran (2025)[34]

This paper explicitly addresses voice assistants within the Indian law by emphasising that even though the DPDP Act is a sound law on paper, ambient recordings are explicitly not covered by this legal framework. Her point plays a vital role in drawing attention to the silence in the doctrines concerning the ambient data. Nevertheless, her paper is limited to identifying the gap. It lacks a technical foundation and fails to offer specific reforms, except general appeals to strengthen defences. This paper addresses those gaps and builds on Sheoran's work by combining technical information about computer science and statutory interpretation. Specifically, this paper proposes explicit amendments defining "ambient data" and mandating on-device processing, which will transform the doctrinal critique of the theory into the practical reform.

IV. CRITICAL ANALYSIS OF THE DPDP ACT AND AMBIENT VOICE DATA

India celebrated the Digital Personal Data Protection Act, 2023 (DPDP Act)[35] as a long-awaited reaction to the Supreme Court of India's acknowledgment of privacy as a fundamental right in K.S. Puttaswamy v. Union of India[36]. Theoretically, the Act incorporates constitutional values of autonomy, dignity, and informational self-determination into statutory protections. Its regulations on consent, purpose restriction, and fiduciary duty resemble international regulations, like the GDPR[37]. However, when applied to the innovative issue of ambient voice information recorded by virtual assistants, the Act shows not only silences in the doctrine but also functional weaknesses. This section critically examines three dimensions: consent under Section 6, processing regulations in Section 7, and the fiduciary duties under Section 8[38].

1. Section 6 and the Fiction of Meaningful Consent

Consent is the key to the DPDP Act. Section 6 requires that personal data processing must be made on the basis of free, specific, informed, unconditional, and unambiguous consent with clear affirmative action[39]. On its part, this criterion seems strict. However, it folds into legal fiction when it is faced with the realities of ambient data. For example, the 2017 Google Super

[34] Sheoran, *supra* note 18, at 23–24.
[35] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[36] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[37] Regulation (EU) 2016/679, *supra* note 11.
[38] Digital Personal Data Protection Act, No. 22 of 2023, §§ 6–8 (India).
[39] *Id.* § 6.

Bowl ad unintentionally activated Google Home devices across the country[40]. The involved users had actually consented to the installation of the devices, but had not, and could not, agree to a TV commercial triggering unintended recordings in their living rooms. Another example is Apple's 2025 $95 million settlement for claims that Siri was recording conversations without the consent of the user[41]. Plaintiffs claimed that Siri was mis-triggered on ambient noise, without wake word, "Hey, Siri!" or a button press. This resulted in unintended recordings, which were stored and reviewed by contractors[42]. Although the U.S. court did not rule on liability, the settlement accepted that no inadvertent, passive captures could be defended by a one-time blanket consent at the time of installation[43]. These incidents show the same underlying problem, that is, consent provided upon installation does not extend indefinitely to every unintended capture.

The magnitude of the problem is confirmed with the help of technical research. A survey conducted by Li and colleagues revealed that 40% of the reported privacy events were false wake-word activations[44]. The user rarely knows when this happens, and even where such a log exists, it is hidden in a dashboard that is rarely visited. Abdi, Ramokapane, and Such showed that due to the common illusion that most users have about how turning a device off terminates all recording, consent under these circumstances cannot be informed and unambiguous[45].

Advocates of the current framework contend that Section 6 already applies by clicking "I agree" during setup, consenting to the danger of occasional misfires. This represents a contractual interpretation of consent, which mirrors industry discourse that privacy is a trade-off for convenience. Such interpretation, however, brings consent down to boilerplate formalism, not linked to the experience of users.

Ambient recordings, as Sheoran has put it, are categorically distinct since they arise outside the volition zone[46]. The right to privacy, as acknowledged in Puttaswamy, is not the allocation of risk in transactions but the maintenance of autonomy and dignity against passive surveillance[47]. Thus, the DPDP Act has to be revised to clearly specify ambient data and mandate persistent,

[40] *Google Super Bowl Ad Inadvertently Triggers Voice-Activated Google Home Speakers*, *supra* note 2.
[41] *Apple's $95 Million Siri Settlement Explained*, *supra* note 5.
[42] *Lopez v. Apple Inc*., No. 5:19-cv-04577 (N.D. Cal. Sept. 5, 2025).
[43] *Id.*
[44] Li et al., *supra* note 33, at 9–12.
[45] Abdi et al., *supra* note 31, at 97–99.
[46] Sheoran, *supra* note 18, at 23–24.
[47] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

event-related consent by real-time alerts.

2. Section 7 and Elasticity of Purpose Limitation

Section 7 limits processing of data collected by Data Fiduciaries to the purposes for which consent was given or otherwise justified under the law[48]. Although a fundamental component of data protection, it is susceptible to abuse due to its elastic nature. Manufacturers often use "service improvement" to justify the processing of ambient recordings.

This issue is exemplified by the Apple Siri settlement case. As part of the terms, Apple agreed to restrict human review of mis-triggered recordings, emphasising how "service improvement" was being extended disproportionately, compared to users' understanding of consent[49]. Similarly, in Wilcosky v. Amazon.com, a U.S. federal court held that indefinite retention of users' voiceprints of Alexa without explicit consent violated Illinois' Biometric Information Privacy Act (BIPA)[50]. In Tice v. Amazon.com, the court permitted claims under the Invasion of Privacy Act in California, noting that unprompted voice recordings can amount to criminal wiretapping[51]. Both cases demonstrate that U.S. courts treat "ambient captures" as distinct from ordinary data and will not permit an elastic corporate defence of breaching user privacy for "product improvement".

Google has admitted using such data to improve speech recognition, and Amazon has utilised contractor reviews to improve Alexa performance[52]. On the surface, these uses may appear aligned with user expectations of product improvement. However, research indicates that there is a difference between corporate framing and consumer perception. Online reviews evaluated by Chhetri and Motti frequently express fear that "the device is listening all the time", reflecting a belief that such processing exceeds acceptable boundaries[53].

Section 7 is also weakened by the opaqueness of processing. After data is uploaded, users, or even regulators, can hardly determine whether the ambient data was processed for personalisation, ensuring quality, or training algorithms. Jemima condemns this opaqueness by pointing out that wide categories of "legitimate use" offer protection to practices that would

[48] Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).
[49] *Lopez v. Apple Inc*., No. 5:19-cv-04577 (N.D. Cal. Sept. 5, 2025).
[50] *Wilcosky v. Amazon.com, Inc*., No. 1:19-cv-05061, 2021 WL 184052 (N.D. Ill. Feb. 5, 2021).
[51] *Tice v. Amazon.com, Inc.,* No. 5:19-cv-1311-SVW-KK, 2020 WL 1283283 (C.D. Cal. Mar. 25, 2020).
[52] Albayaydh & Flechais, *supra* note 8, at 2–3.
[53] Chhetri & Motti, *supra* note 32, at 248–50.

otherwise breach purpose limitation[54].

Counter-arguments by the Data Fiduciaries emphasise that limiting processing would be counterproductive to innovation. They argue that without analysing real-world mis-triggered data, they cannot improve wake-word accuracy, leaving the devices error-prone and frustrating to customers. In this light, India's digital economy may be harmed if the DPDP Act restricts the data-driven development of AI assistants.

This is a valid concern, yet it represents a false dichotomy between rights and innovation. Loideain and Adams posit in the GDPR context that technological progress must operate within boundaries that preserve trust[55]. Thus, on-device processing can be a reasonable compromise, as the wake-word accuracy can be enhanced locally without ambient data being sent to the cloud. This would preserve innovation while respecting the principle of purpose limitation under Section 7 of the DPDP Act[56].

3. Section 8 and Hollow Promises of Fiduciary Responsibility

Section 8 imposes a broad set of obligations on Data Fiduciaries to ensure safeguards, prevent breaches, and enforce compliance[57]. By transforming companies into fiduciaries, the Act aims to expand corporate duties and obligations beyond a contract and place them under quasi-trustee obligations. However, in the case of voice assistants, such safeguards collapse due to a lack of transparency and enforcement.

According to the interviews conducted by Abdi et al., users have grossly misconceived how voice assistants operate and believe that muting prevents recording or that a deletion command removes all stored information[58]. These misconceptions are not only a matter of user ignorance but evidence of opaque design. If fiduciary were acting in data principal's best interest, transparency would be built into the device interface and not embedded in inaccessible dashboards.

---

[54] B.S. JEMIMA, BALANCING THE GROWTH OF E-COMMERCE WITH DATA SECURITY AND PRIVACY: AN ANALYSIS OF THE INDIAN LEGISLATIVE FRAMEWORK 41–42 (2025).
[55] NORA NI LOIDEAIN & RACHEL ADAMS, *From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments*, 36 COMPUTER L. & SEC. REV. 105397, 105400–02 (2019) DOI: 10.1016/j.clsr.2019.105366.
[56] Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).
[57] *Id.* § 8.
[58] Abdi et al., *supra* note 31, at 100–02.

The practice in the United States supports the need for voluntary disclosure. In re Google Assistant Privacy Litigation, the court emphasised user autonomy by permitting class members to reject a settlement and bring individual cases[59]. This is an institutional acknowledgement that privacy remedies must preserve meaningful user choice. Similarly, Apple had to modify its practices, not just pay damages in the Siri settlement[60]. These structural solutions imply that fiduciary responsibility should be beyond aspirations and be supported by mandatory measures, such as audits, disclosure, and sanctions.

The evidentiary process of voice data repurposing, makes safeguards even more difficult. In State of New Hampshire v. Verrill[61], a homicide investigation, the trial court in New Hampshire ordered Amazon to surrender Echo recordings. Currently, the DPDP Act does not address the evidentiary uses of unintended recordings, but its omission indicates that there is a risk that such recordings may be exploited by companies and the State, using ambient recordings as a parallel surveillance regime. Unlike GDPR[62], the DPDP Act does not mandate Data Protection Impact Assessments for high-risk technologies like voice assistants. Nor does it mandate disclosure of mis-trigger rates or ambient data-handling independent audits. With no institutionalised means of control, fiduciary rhetoric in the European context collapses, as De Conca notes, into the "trust us" assurances that are not worthy of trust[63].

Counter-arguments suggest that excessive regulation can discourage investment and innovation in the digital economy in India. The voluntary dashboards and self-regulation are adequate examples of corporate responsibility. However, repeated lawsuits demonstrate that voluntary measures are reactive, opaque and ineffective. Thus, Section 8 should be enhanced with mandatory audits, reporting of transparency, and penalties that may be enforced in the instance of non-compliance.

V. COMPARISON OF SAFEGUARDS AGAINST AMBIENT VOICE SURVEILLANCE UNDER GDPR, CPRA AND DPDP

Ambient recordings pose a problem beyond India. The European Union, as well as the United States, has struggled to control voice assistants within its data protection frameworks, showing

[59] *In re Google Assistant Privacy Litigation*, No. 5:19-cv-04286-BLF (N.D. Cal. Feb. 14, 2025).
[60] *Lopez v. Apple Inc*., No. 5:19-cv-04577 (N.D. Cal. Sept. 5, 2025).
[61] *State of New Hampshire v. Verrill*, No. 659-2017-CR-576, Order (Rockingham Cty. Sup. Ct. Dec. 4, 2018).
[62] Regulation (EU) 2016/679, art. 6, *supra* note 11.
[63] De Conca, *supra* note 12, at 5–7.

that they have the same areas of concern as well as a number of unique gaps, which provide valuable lessons in enhancements to the DPDP Act in India.

a. General Data Protection Regulation (GDPR)

GDPR is considered to be the most extensive privacy regime. It states that consent should be free, specific, informed and direct, and processing should be limited to the reasons that were stated to the data subject[64], i.e., the incident involving voice assistants in Europe, where Google contractors reportedly listened to the recording without consent, created regulatory concerns under these clauses[65]. High-risk technology also requires a Data Protection Impact Assessment (DPIA) under the GDPR[66]. Notwithstanding the solid principles, researchers believe that the GDPR is inadequate for ambient data. According to De Conca, continuous listening prevents real-time informed consent, leaving users oblivious to the majority of unwanted activations observable[67]. Loideain and Adams further argue that voluntary disclosures and post-hoc audits fail to protect against the structural opacity of "always listening" devices[68]. Thus, the enforcement of GDPR in the context of ambient data is limited.

b. California Privacy Rights Act (CPRA)

The California Privacy Rights Act (CPRA)[69] gives consumers in the United States the right to access, delete, and opt out of the sale of their personal data. This was used in the class action to enforce these rights, including against Apple over the unintentional recordings made by Siri, resulting in a $95 million settlement in 2025[70].

However, the CCPA is narrower than the GDPR[71]. It frames protections primarily as consumer rights rather than fiduciary obligations, not requiring DPIAs or prior risk assessments. According to scholars, its opt-out framework is not adequate for ambient data, where people might be unaware that they are being recorded[72].

---

[64] Regulation (EU) 2016/679, art. 6, *supra* note 11.
[65] Albayaydh & Flechais, *supra* note 8, at 2–3.
[66] Regulation (EU) 2016/679, art. 35, *supra* note 11.
[67] De Conca, *supra* note 12, at 5–7.
[68] Loideain & Adams, *supra* note 55, at 105400–02.
[69] CAL. CIV. CODE §§ 1798.100–.199 (West 2023).
[70] *Apple's $95 Million Siri Settlement Explained*, *supra* note 5.
[71] Regulation (EU) 2016/679, *supra* note 11.
[72] R. SONG, *Shattering the One-Way Mirror: AI, Data Breaches, and Privacy*, SSRN (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5254316.

c. Implications for India

The DPDP Act of India[73] is more in line with the principles of the GDPR of consent and fiduciary, rather than the consumer-rights approach of the CCPA. Nevertheless, as Jemima and Sheoran note, the Act mimics most of the blind spots of the GDPR in that it does not specifically cover ambient recordings[74]. These inadequacies provide an opportunity for India to explicitly define the concept of ambient data, make the processing on-device mandatory, and conduct proactive audits, so that the shortcomings of both regimes are overcome.

VI. REFORM PROPOSALS

a. Legal Reforms

1. In the Act, the term ambient data should be treated as a different category of personal data, which is not deliberate inputs, but ambiently recorded without any knowledge or purpose[75]. Currently, Sections 6 and 7[76] of the consent and processing permit Data Fiduciaries to use the general installation-stage consent. This loophole would be closed off by a statutory definition under the DPDP Act.[77]

2. Section 6 consent must be dynamic, not inert. Users must be alerted in real-time, when unintentional audio is captured (by the device) through short messages, beeps, and icons[78]. The increased consent levels while high-risk processing under GDPR[79] can offer a helpful framework.

3. The privacy-by-design principle of section 8 should be extended to require ambient clip processing locally. The upload to cloud servers must be done at the user's individual choice. This minimises the chances of data breaches, leaks, and abuse[80].

4. The fiduciary obligations should be met with false activations, annual reports, retention practices, and protection. Voice-assistant manufacturers should be obligated to undergo

[73] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[74] Jemima, *supra* note 54, at 41–42; Sheoran, *supra* note 18, at 23–24.
[75] E. HÄRDLING, DATA PROTECTION IN THE SMART HOME: DO DATA SUBJECTS HAVE CONTROL OVER AI-GENERATED INFERENCES? 45–46 (2022) (Master's Thesis, Uppsala University).
[76] Digital Personal Data Protection Act, No. 22 of 2023, §§ 6–7 (India).
[77] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[78] Abdi et al., *supra* note 31, at 97–99.
[79] Regulation (EU) 2016/679, art. 6, *supra* note 11.
[80] De Conca, *supra* note 12, at 5–7.

independent audits, which are based on GDPR Data Protection Impact Assessments[81]. This will improve accountability and transparency.

b. Manufacturer Reforms

1. Developing Wake-Word Accuracy, as research indicates that almost 40 percent of accidental records are because of a false activation[82]. The unnecessary surveillance is lowered through investment in an improved wake-word detection.

2. Most users do not possess proper mental modes of how devices should behave. Status recording should be easy through persistent indicators, on the device itself, such as LEDs or spoken alerts.

3. The default retention value of ambient clips should be short (e.g. 24 hours), unless otherwise specified by users. Eliminating the data automatically reduces corporate misuse and complies with the data minimization norms[83].

c. Consumer Reforms

1. Clearer Setup Instructions as mute switch or indicators are usually misinterpreted by consumers[84]. The manufacturers are required to give straightforward explanations concerning when the devices listen and how the controls work.

2. Standardised dashboards should allow users to review and delete recordings, including accidentally captured ones, with ease. The present ones are opaque and confusing.

3. Digital privacy literacy and responsible device use should become the new normal through government and civil society campaigns like seatbelt awareness campaigns.

d. Bystander Protections

Voice assistants capture non-users (family members, guests, or workers entering homes) on a regular basis. These people are seldom willing to consent, and this is a concern to privacy as

[81] Regulation (EU) 2016/679, art. 6, *supra* note 11.
[82] Li et al., *supra* note 33, at 9–12.
[83] Jemima, supra note 54, at 41–42.
[84] Chhetri & Motti, *supra* note 32, at 248–50.

well as constitutionality[85]. Thus -

1. The speech by bystanders should be anonymized unless permission is given.

2. The bystanders should be allowed to exclude themselves with the help of simple commands like do not record.

3. The DPDP Act[86] should be amended to emphasise that fiduciary duties are applicable to all the people affected, and not only to the registered users.

e. Ecosystem Reforms

1. The Data Protection Board should be able to audit, require transparency and enforce meaningful punishment on offenders.

2. Self-regulation should give way to government-supported technical standards on the accuracy of wake words and deletion protocols as well as local processing. Certification schemes may provide assurance to the consumers.

VII. CONCLUSION

This paper has undertaken a critical analysis to establish the effectiveness of the Digital Personal Data Protection (DPDP) Act, 2023[87] in addressing the privacy threat posed by ambient voice recordings from voice assistants. The main findings show that, as much as the Act is a legislative landmark, its provisions are inadequate to address the threat of unintentional data capture, which is by always-on devices. As a result, a strong disparity still exists between the aims of the Act and its actual ability to protect citizens in their rights to privacy against this type of modern surveillance.

The analysis indicates that the core principles of the Act, which are consent, limitation of purpose, and the duty of fiduciaries, are structurally weak in relation to ambient data. The consent principle of Section 6[88] is essentially defeated, and a single time consenting to the installation of the device cannot be reasonably interpreted as a lifetime agreement to have

[85] Albayaydh & Flechais, *supra* note 8, at 2–3.
[86] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[87] *Id.*
[88] *Id.* § 6.

sensitive conversations perpetually captured, especially without the user's knowledge. Similarly, the doctrine of purpose limitation in Section 7[89] is excessively flexible. Data Fiduciaries justify the processing of ambiently collected data by vague reasons such as improvement in the service, thereby processing beyond the original purpose and the user's reasonable expectation, violating the provision. Moreover, the fiduciary obligations of Section 8[90] show an absence of enforcement mechanisms, which makes the fiduciary duty to serve the interests of the data principal unenforceable.

The study of similar international systems, such as the General Data Protection Regulation[91] by the European Union, and the California Privacy Rights Act in California[92], indicates that the regulatory gap on ambient data is a transnational problem. To rectify the shortcomings and practically achieve the constitutional privacy as expressed in K.S. Puttaswamy v. Union of India[93], the paper suggests reforms.

These include the creation of a statutory definition of ambient data, the introduction of on-device processing as a default option, the introduction of dynamic consent processes in the form of real-time notifications, the introduction of compulsory independent auditing, and the expansion of legal protections to bystanders.

To conclude, the social advantages of the voice-activated technologies should be balanced with the social right of privacy and digital dignity that cannot be negotiable. As it currently exists, the DPDP Act allows technology to overstep the basic legal safeguards. Thus, it is necessary to take practical steps as aforementioned, so that the legislature will be able to create a reasonable balance between innovation and the preservation of constitutional rights, especially in the digital age, making technology an assistant to humanity, but not its destroyer.

[89] *Id.* § 7.
[90] *Id.* § 8.
[91] Regulation (EU) 2016/679, *supra* note 11.
[92] CAL. CIV. CODE § 1798.100 *et seq.* (West 2023).
[93] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.