



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

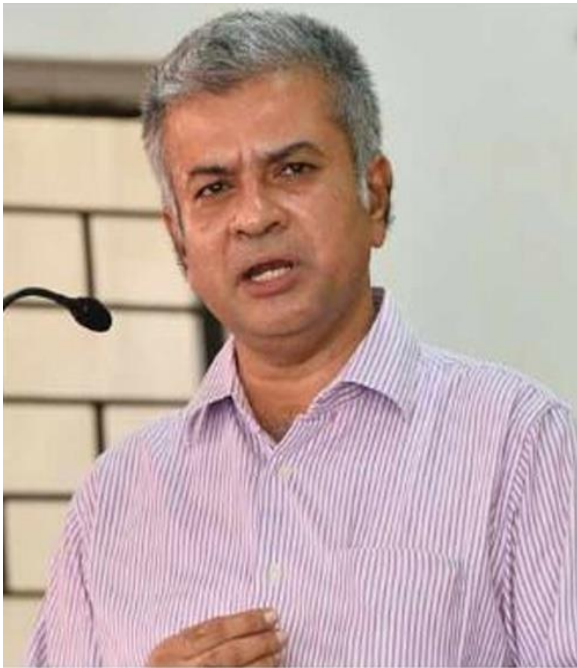
DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



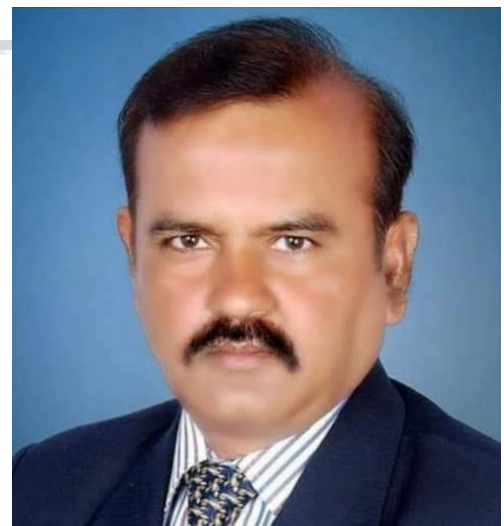
Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

diploma in Public

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

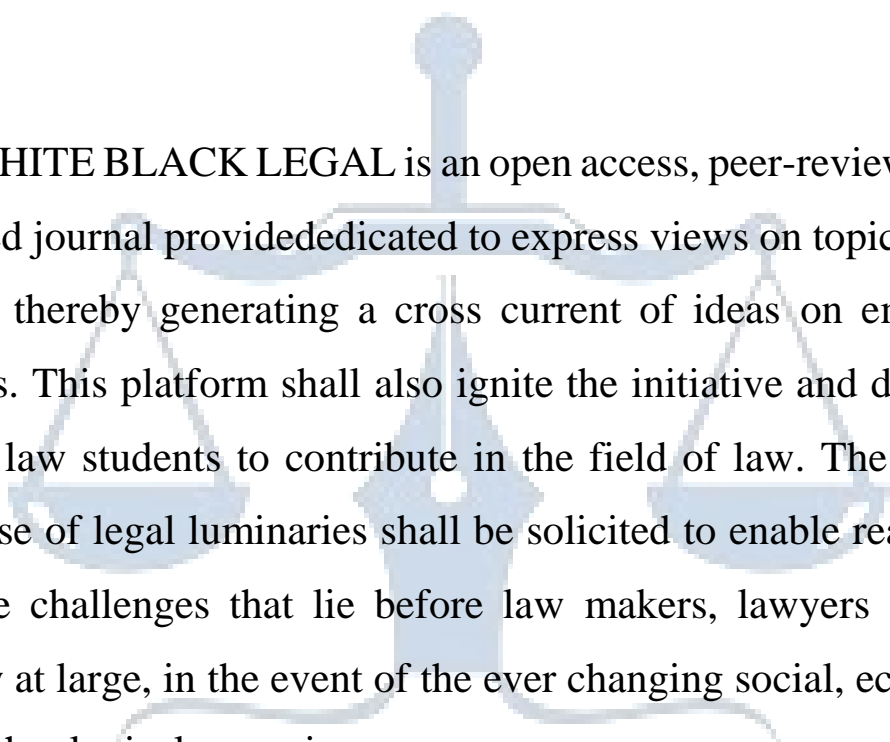


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

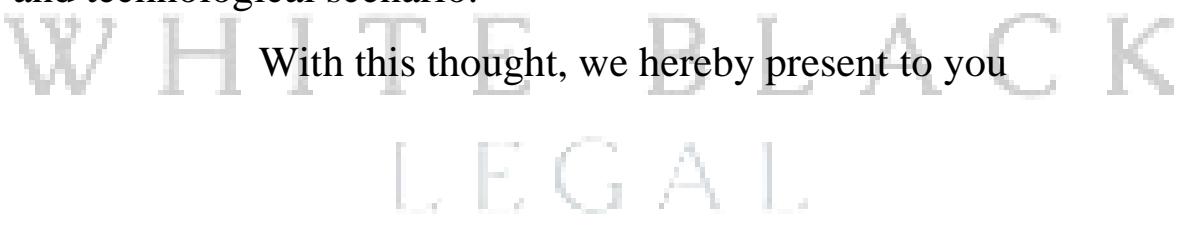
Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you



VOICE ASSISTANTS AND DATA SECURITY: NAVIGATING ETHICAL AND LEGAL CONCERNS

AUTHORED BY - SUCHITRA SHEORAN

Introduction

The Fourth Industrial Revolution has brought about a profound transformation in how humans interact with technology.¹ At the forefront of this change are voice assistants (VAs) like Amazon's Alexa, Google Assistant, Apple's Siri, and Microsoft's Cortana, which have become ingrained in our daily routines.² By enabling hands-free operation through voice commands, these technologies offer unparalleled convenience, integrating seamlessly into devices ranging from smartphones to home appliances.³ As society embraces the ease of use that voice assistants provide, it is evident that this technology has quickly moved from novelty to necessity.

Numerous studies and market data reflect the widespread adoption of voice assistants. A 2018 PwC survey analysed 1,000 American respondents aged 18-64, revealing that 90% of the participants were familiar with voice-controlled devices, and 72% actively used them.⁴ Of these, 57% utilised VAs on smartphones, 29% on laptops, and 27% on smart speakers.⁵ Furthermore, despite potential privacy risks, 44% users employed VAs to control their other devices by integrating their entire digital ecosystem, from smart home systems to connected financial accounts.⁶ But, a smaller segment, i.e. about 9%, expressed no interest in using voice assistants, emphasising the tension between convenience and privacy.⁷

¹ See, e.g., Bernard Marr, *Why Everyone Must Get Ready For The 4th Industrial Revolution*, FORBES, <https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/> (last visited Oct 16, 2024).

² Parker Hall & Nena Farrell, *10 Best Smart Speakers (2024): Alexa, Google Assistant, Siri* | WIRED, <https://www.wired.com/story/best-smart-speakers/> (last visited Oct 18, 2024).

³ See, e.g., Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL STREET JOURNAL, Jan. 4, 2015, <http://online.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511> (last visited Oct 16, 2024).

⁴ PricewaterhouseCoopers, *Consumer Intelligence Series: Prepare for the Voice Revolution*, PWC, <https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/voice-assistants.html> (last visited Oct 16, 2024).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

On a global scale, the voice technology market has shown a remarkable growth. In India, voice searches has increased by 270% year-on-year in 2020, with 60% of the total users regularly interacting with voice assistants.⁸ Smart speakers, as noted in the Mobile Marketing Association's 2021 Voice Playbook, have become essential household tools due to their VA integration.⁹ Worldwide, the number of digital voice assistants rose from 3.25 billion in 2019 to 4.2 billion in 2020, with projections estimating that by 2024, there will be 8.4 billion devices equipped with VAs—exceeding the global population.¹⁰ The global voice market, valued at USD 10.7 billion in 2020, is expected to reach USD 27.15 billion by 2026, growing at a compound annual growth rate (CAGR) of 16.8%.¹¹

However, as voice assistants have become more ingrained in our lives, they raise complex privacy and data security concerns. By their inherent design, these devices continuously listen for activation commands, making them vulnerable to collecting and misusing personal data. Such concerns have prompted regulators and lawmakers to take action, particularly with the introduction of frameworks like the European Union's General Data Protection Regulation (GDPR)¹² and India's Digital Personal Data Protection (DPDP) Act.¹³ These regulations seek to protect users by ensuring that companies collecting data adhere to strict guidelines regarding consent, transparency, data minimisation, etc. But, as VAs evolve and become part of everyday life, the sufficiency of these regulatory frameworks is being questioned.

In this context, it becomes imperative to evaluate whether the DPDP Act of 2023 is adequately equipped to manage the data security challenges posed by voice assistants in India. A comparative analysis with the GDPR, which has been at the forefront of global data protection efforts, can offer valuable insights. Understanding how the GDPR addresses the risks associated with voice assistants and examining the extent to which the DPDP Act aligns with or diverges from these standards is crucial in determining whether India's regulatory framework can effectively safeguard personal data in this new era. Moreover, by identifying areas where

⁸ Year in Search — India: Insights for brands, THINK WITH GOOGLE, <https://www.thinkwithgoogle.com/intl/en-apac/marketing-strategies/search/year-in-search-india-insights/> (last visited Oct 15, 2024).

⁹ The Voice Playbook 2021, MMA GLOBAL, <https://www.mmaglobal.com/documents/voice-playbook-mma-ammpp-voice-audio-initiative> (last visited Oct 15, 2024).

¹⁰ Number of voice assistants in use worldwide 2019-2024, STATISTA, <https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/> (last visited Oct 18, 2024).

¹¹ The Voice Playbook 2021, *supra* note 9.

¹² The General Data Protection Regulation (GDPR) is European Union legislation enacted to enhance and unify data privacy laws across the EU, replacing the 1995 Data Protection Directive. It came into effect on May 25, 2018, to safeguard personal data and ensure responsible handling of such information by organisations.

¹³ The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.

the DPDP Act may benefit from the GDPR's robust approach, this paper seeks to explore how India's evolving data protection regime can be strengthened to meet the growing concerns around privacy in the context of voice assistants.

This paper explores the dual nature of voice assistants—their functionality and convenience in the first section versus the data security risks they pose in the second section. The third section will compare the GDPR with India's DPDP Act, analysing how these regulations address data privacy in the context of VAs and how GDPR might serve as a model for strengthening India's evolving legal framework.

Voice Assistants and their Functionality

Voice assistants (VAs) are a sophisticated category of artificial intelligence systems that allow users to interact with technology using natural spoken language.¹⁴ These digital companions, embedded in devices such as smartphones, smart speakers, laptops, and even automobiles, have become integral to everyday life, providing a seamless and efficient way to execute tasks.¹⁵ By recognising and processing voice commands, VAs can perform various functions, from setting reminders and controlling home appliances to offering personalised recommendations and streaming entertainment.

At the core of voice assistants' functionality is **speech recognition technology**, which enables the devices to "listen" to user commands.¹⁶ This technology has evolved significantly since its inception in the 1960s when IBM's Shoebox was introduced, capable of recognising just sixteen words.¹⁷ Today, voice assistants, powered by advanced AI algorithms, can detect and interpret a wide variety of complex speech inputs with remarkable accuracy. For example, Google Assistant, one of the leading VAs, can recognise 19 out of 20 words it hears.¹⁸ Such accuracy

¹⁴ SmartSites, *What Is a Digital Assistant?*, LIBRESTREAM (Jul. 11, 2024), <https://librestream.com/blog/what-is-a-digital-assistant/> (last visited Oct 16, 2024).

¹⁵ Alexa, *Do You Have Rights? Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, https://www.americanbar.org/groups/business_law/resources/business-law-today/2017-july/alex-a-do-you-have-rights/ (last visited Oct 16, 2024).

¹⁶ Anna Karapetyan, *DEVELOPING A BALANCED PRIVACY FRAMEWORK*, 27 SOUTHERN CALIFORNIA REVIEW OF LAW AND SOCIAL JUSTICE 197 (2018).

¹⁷ Ava Mutchler, *A Timeline of Voice Assistant and Smart Speaker Technology From 1961 to Today*, VOICEBOT.AI (2018), <https://voicebot.ai/2018/03/28/timeline-voice-assistant-smart-speaker-technology-1961-today/> (last visited Oct 18, 2024).

¹⁸ Bernard Marr, *Machine Learning In Practice: How Does Amazon's Alexa Really Work?*, FORBES, <https://www.forbes.com/sites/bernardmarr/2018/10/05/how-does-amazons-alexa-really-work/> (last visited Oct 18, 2024).

reflects years of technological advancement in **automatic speech recognition (ASR)**¹⁹ and **natural language processing**.

Voice assistants typically function by responding to specific "**wake words**"—phrases like "Hey Siri" or "Ok Google"—that activate the device.²⁰ Once activated, the device begins recording the user's voice command and transmits the audio data to the cloud for processing.²¹ This is where the power of AI and machine learning comes into play: the spoken words are converted into text and then interpreted to determine the user's intent using **natural language understanding (NLU)** algorithms.²² Based on this understanding, the assistant generates an appropriate response, ranging from answering a question to controlling connected smart devices like thermostats or lights.²³

Once the voice command is processed, the VA sends the response back to the device, which communicates the answer through **text-to-speech (TTS)** technology, allowing the user to hear the response.²⁴ For instance, if a user asks, "What's the weather like today?" the voice assistant will process the question, retrieve relevant data from the internet, and deliver a spoken response like "The weather today is sunny with a high of 25 degrees." This entire process happens in seconds, making the interaction feel smooth and intuitive.

¹⁹ Automatic Speech Recognition (ASR), also known as speech-to-text, is the process by which a computer or electronic device converts human speech into written text. This technology is a subset of computational linguistics that deals with the interpretation and translation of spoken language into text by computers. It enables humans to speak commands into devices, dictate documents, and interact with computer-based systems through natural language. See Automatic Speech Recognition, DEEPAI (2019), <https://deepai.org/machine-learning-glossary-and-terms/automatic-speech-recognition> (last visited Oct 18, 2024).

²⁰ Alexa and Alexa Device FAQs - Amazon Customer Service, <https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230> (last visited Oct 18, 2024); Choose Google Home: Seamless Control Enhanced Features for Your Home, <https://home.google.com/about-google-home/> (last visited Oct 18, 2024); Rowan Trollope, *7 Things You Didn't Know About Wake Words*, MEDIUM (Nov. 29, 2017), <https://medium.com/@rowantrollope/7-things-you-didnt-know-about-wake-words-d4e9e041d11d> (last visited Oct 18, 2024).

²¹ Jurriaan Van Mil & João Pedro Quintais, *A Matter of (Joint) Control? Virtual Assistants and the General Data Protection Regulation*, 45 COMPUTER LAW & SECURITY REVIEW 105689 (2022).

²² Natural language understanding (NLU) is an aspect of natural language processing (NLP) that focuses on how to train an artificial intelligence (AI) system to parse and process spoken language in a way that is not exclusive to a single task or a dataset. See Natural Language Understanding (NLU), TECHOPEDIA (Dec. 9, 2021), <https://www.techopedia.com/definition/33013/natural-language-understanding-nlu> (last visited Oct 18, 2024).

²³ Van Mil and Quintais, *supra* note 21.

²⁴ Luca Hernández Acosta & Delphine Reinhardt, *A Survey on Privacy Issues and Solutions for Voice-Controlled Digital Assistants*, 80 PERVASIVE AND MOBILE COMPUTING 101523 (2022).

Beyond simple tasks like answering questions, setting reminders, or playing music, VAs are increasingly becoming integral to the **Internet of Things (IoT)**.²⁵ Modern homes are often equipped with multiple smart devices that can be controlled through voice commands. For instance, users can ask their voice assistant to turn off lights, adjust the thermostat, or even start a washing machine. Companies like LG,²⁶ Samsung, Hyundai²⁷ and Ford²⁸ have integrated voice assistants into home appliances and vehicles, making it possible to control a wide array of devices through simple voice commands. This has created a truly **connected ecosystem**, where users can manage various aspects of their homes or cars simply by speaking.

Voice assistants are also designed to improve over time by learning from user interactions. This is achieved through **machine learning algorithms**, which allow the system to refine its responses and understand user preferences based on past behaviour.²⁹ For example, Amazon's Alexa continuously learns from user commands to enhance its understanding of individual speech patterns and preferences.³⁰ This learning process allows the assistant to offer more accurate responses and recommendations as it becomes more attuned to the user's needs.

Moreover, voice assistants are not restricted to English-speaking users. In countries like India, where linguistic diversity is vast, voice assistants are being designed to support multiple languages. By 2021, it was estimated that 72% of Indian users would prefer interacting with voice assistants in languages other than English, reflecting the growing role of VAs in making

²⁵ Nicole Kobie, *What Is the Internet of Things?*, THE GUARDIAN, May 6, 2015, <https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google> (last visited Oct 18, 2024).

²⁶ Amazon's Alexa assistant is coming to LG refrigerators, <https://www.engadget.com/2017-01-04-lg-refrigerator-with-amazons-alexia.html> (last visited Oct 18, 2024).

²⁷ Amazon Staff, *Amazon and Hyundai Launch a Broad, Strategic Partnership—Including Vehicle Sales on Amazon.Com in 2024*, (2023), <https://www.aboutamazon.com/news/company-news/amazon-hyundai-partnership> (last visited Oct 18, 2024).

²⁸ Ford Assistant And Voice Commands With Sync® 4a | 2022 Ford Mustang Mach-E Videos | Ford Owner Support, <https://www.ford.com/support/vehicle/mustang-mach-e/2022/how-to-videos/video-library/sync/6317860956112?name=ford-assistant-and-voice-commands-with-sync-4a> (last visited Oct 18, 2024).

²⁹ Jessica D. Cox, "ALEXA, ARE YOU LISTENING?" USING CARPENTER AND TRADITIONAL PROPERTY-BASED FOURTH AMENDMENT ANALYSES TO DETERMINE HOW VOICE ASSISTANT DATA CAN BE PROTECTED UNDER THE FOURTH AMENDMENT, 44 OKLAHOMA CITY UNIVERSITY LAW REVIEW 117 (2019).

³⁰ Marissa Merrill, *An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*, 71 MERCER LAW REVIEW 637 (2020).

technology more accessible to a wider audience.³¹ Gaana's³² expansion into rural India, with the addition of voice search functionality, has helped overcome literacy barriers for new internet users.³³ In just one year, **24%** of its users began using voice search, reflecting the growing accessibility and ease of use for this audience.³⁴

Concerns Surrounding Voice Assistants

Voice assistants (VAs), while offering significant convenience and seamless integration into everyday life, have raised numerous privacy and data security concerns. These concerns revolve around the ability of VAs to collect, store, and process vast amounts of personal data—often without explicit user consent or awareness. The primary concerns associated with voice assistants include:

1. *Unintended Data Collection*

Voice assistants are designed to respond to specific wake words but are always in listening mode, which can sometimes be triggered accidentally. This phenomenon, known as a "false positive,"³⁵ occurs when a VA misinterprets random conversation as a command. For instance, in 2018, Amazon Alexa accidentally recorded a private conversation and sent it to a random contact.³⁶ While Amazon stated that this was an isolated incident, it highlights the potential for unintended data collection and privacy breaches.

In another case involving Samsung Smart TVs, the company warned users that conversations near the TV could be recorded and transmitted to third-party servers.³⁷ This raised concerns about whether users were adequately informed about the privacy implications of owning voice-activated devices.³⁸

³¹ How is voice making technology more accessible in India?, THINK WITH GOOGLE, <https://www.thinkwithgoogle.com/intl/en-apac/future-of-marketing/emerging-technology/ok-google-how-is-voice-making-technology-more-accessible-in-india/> (last visited Sep 23, 2024).

³² India's music streaming service.

³³ How is voice making technology more accessible in India?, *supra* note 31.

³⁴ *Id.*

³⁵ Amazon has a fix for Alexa's creepy laughs - The Verge, <https://www.theverge.com/circuitbreaker/2018/3/7/17092334/amazon-alexa-devices-strange-laughter> (last visited Oct 18, 2024).

³⁶ Amazon explains how Alexa recorded a private conversation and sent it to another user - The Verge, <https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation> (last visited Oct 18, 2024).

³⁷ Your Samsung TV is eavesdropping on your private conversations, <https://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html> (last visited Oct 18, 2024).

³⁸ *Id.*

Voice assistants (VAs) are designed to activate upon detecting specific wake words; however, studies indicate that they can be triggered by similar-sounding phrases. For example, terms like "unacceptable" and "tobacco" have inadvertently activated Amazon's Alexa and Google Home, raising concerns about accidental recordings.³⁹ A study found that **64%** of users experienced unintentional activations at least once a month, highlighting the frequency of potential privacy invasions.⁴⁰ A notable incident with the Google Home Mini involved continuous recordings due to a hardware malfunction, occurring even when the wake word was not spoken.⁴¹ This situation underscores the inherent risks of passive, always-listening devices and their potential to compromise user privacy.

2. *Data Retention and Storage*

Voice assistants store user data to improve functionality, but questions arise about how long it is retained and how securely it is stored. In a data breach, sensitive information, including voice recordings, could be exposed to malicious actors.⁴² Furthermore, storing user data on cloud servers presents additional security risks, as cloud infrastructures can be vulnerable to hacking.⁴³ Amazon, in one case, didn't delete the data even after a user requested it.⁴⁴

In 2018, Amazon faced a significant privacy breach when a user requested his own data, and Amazon sent 1700 Alexa recorded audio files belonging to another user.⁴⁵ The incident raised questions about Amazon's data handling practices and whether they complied with GDPR. The company claimed that the breach resulted from human error, but it led to increased scrutiny of how voice assistants process and store user data.

³⁹ Uncovered: 1,000 phrases that incorrectly trigger Alexa, Siri, and Google Assistant - Ars Technica, <https://arstechnica.com/information-technology/2020/07/uncovered-1000-phrases-that-incorrectly-trigger-alex-siri-and-google-assistant/> (last visited Oct 18, 2024).

⁴⁰ Eric Hal Schwartz, *Voice Assistants Accidentally Awakened by 64% of Users a Month: Survey*, VOICEBOT.AI (2020), <https://voicebot.ai/2020/01/09/voice-assistants-accidentally-awakened-by-64-of-users-a-month-survey/> (last visited Oct 18, 2024).

⁴¹ Dieter Bohn, *Google's Home Mini Needed a Software Patch to Stop Some of Them from Recording Everything* - The Verge, <https://www.theverge.com/2017/10/10/16456050/google-home-mini-always-recording-bug> (last visited Oct 18, 2024).

⁴² Merrill, *supra* note 30.

⁴³ *Id.*

⁴⁴ Amazon's Echo for Kids Violated Privacy Law, Advocacy Groups Say, BLOOMBERG.COM, May 9, 2019, <https://www.bloomberg.com/news/articles/2019-05-09/amazon-s-echo-for-kids-violated-privacy-law-advocacy-groups-say> (last visited Oct 18, 2024).

⁴⁵ Holger Bleich, *Alexa, Who Has Access to My Data?: Amazon Reveals Private Voice Data Files*, INVESTIGATIVE ALEXALEAKS, https://www.heise.de/downloads/18/2/5/6/5/3/9/6/ct.0119.016-018_engl.pdf.

3. *Human Review of Sensitive Data*

To enhance the functionality of voice assistants, companies employ human contractors to review recorded audio for accuracy and to improve voice recognition capabilities.⁴⁶ Despite assurances of anonymisation, numerous reports have surfaced indicating that reviewers frequently overheard sensitive information, including private conversations and personal details.⁴⁷ In 2019, it was reported that Apple contractors often encountered confidential medical discussions and personal information while analysing audio clips.⁴⁸ Such exposure of private moments without user consent significantly undermines trust in these technologies.

In 2019, the Data Protection Commission in Ireland launched an investigation into Google for processing voice data without obtaining proper consent from users.⁴⁹ This followed revelations that Google employed human reviewers to analyse voice recordings from its Assistant service.⁵⁰ The investigation highlighted the need for greater transparency in how voice assistants collect and use data, and Google subsequently halted its human review process to comply with GDPR.⁵¹

4. *Vulnerability to Hacking and Surveillance*

The constant connectivity of voice assistants to the internet makes them susceptible to hacking and cybersecurity risks. For example, the "Dolphin attack" exploits inaudible ultrasonic commands to manipulate devices, allowing unauthorised actions to be performed without the user's knowledge.⁵² Additionally, features such as Amazon Echo's "Drop-In" allow for remote listening, which malicious actors or abusive individuals could misuse.⁵³ This capability raises critical privacy concerns akin to wiretapping, emphasising the need for robust security measures to protect users.

⁴⁶ Nicole Nguyen, *A Team At Amazon Is Listening To Recordings Captured By Alexa*, BUZZFEED NEWS (2019), <https://www.buzzfeednews.com/article/nicolenguyen/amazon-employees-listening-to-alexa-echo-recordings> (last visited Oct 18, 2024).

⁴⁷ *Id.*

⁴⁸ Apple contractors "regularly hear confidential details" on Siri recordings | Apple | The Guardian, <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings> (last visited Oct 18, 2024).

⁴⁹ Rory Carroll & Rory Carroll Ireland correspondent, *Google Faces Irish Inquiry over Possible Breach of Privacy Laws*, THE GUARDIAN, May 22, 2019, <https://www.theguardian.com/world/2019/may/22/irish-statutory-inquiry-to-investigate-if-google-flouted-privacy-laws> (last visited Oct 18, 2024).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Hernández Acosta and Reinhardt, *supra* note 24.

⁵³ Alexa Drop In, Calling, Intercom and Announcements | Amazon.com, <https://www.amazon.com/alexa-drop-in-calling-intercom/b?ie=UTF8&node=21393410011> (last visited Oct 18, 2024).

In a notable 2012 case, hackers remotely accessed Samsung Smart TVs, enabling them to spy on users by activating the device's camera and microphone.⁵⁴ This incident illustrates the potential for voice assistants to be exploited as tools for surveillance, whether by malicious actors or governments.

5. ***Profiling and Targeted Advertising***

Another concern is the use of data collected by voice assistants for profiling and targeted advertising.⁵⁵ Companies often use voice data to create detailed profiles of users, which can then be monetised through personalised advertising.⁵⁶ For example, data brokers can aggregate information from multiple sources, creating detailed profiles of users that include both their online and offline behaviours.⁵⁷ This wealth of information can be exploited by third parties for targeted advertising or surveillance, raising ethical concerns about how such data is used without explicit user consent.⁵⁸

6. ***Children's Privacy***

Children's privacy is also at risk when using voice assistants. Devices such as internet-connected toys, speech-mimicking gadgets and smart speakers in homes often collect data from minors who may not fully understand the implications of privacy.⁵⁹ In 2017, for instance, over two million voice recordings from a children's toy were exposed due to inadequate security protections.⁶⁰ These recordings, which included conversations between children and their parents, were accessed by unauthorised third parties.⁶¹ Such incidents underscore the vulnerability of young users and highlight the need for more stringent regulations to protect children's data.

⁵⁴Your TV might be watching you, <https://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html> (last visited Oct 18, 2024).

⁵⁵Lindsey Barrett & Ilaria Liccardi, *Accidental Wiretaps: The Implications of False Positives by Always-Listening Devices for Privacy Law & Policy*, 74 OKLAHOMA LAW REVIEW 79 (2022).

⁵⁶*Id.*

⁵⁷James Wilson, *What Are Data Brokers and Why Do They Have My Data?*, MY DATA REMOVAL, <https://www.mydataremoval.com/blog/what-are-data-brokers/> (last visited Oct 19, 2024).

⁵⁸Ibekie, *What Are Data Brokers Doing with Your Personal Information?*, MY DATA REMOVAL (2024), <https://www.mydataremoval.com/blog/what-are-data-brokers-doing-with-your-personal-information/> (last visited Oct 19, 2024).

⁵⁹Eric Boughman & Michael V Silvestro, "Alexa, Do You Have Rights?," BUSINESS LAW TODAY 1 (2017).

⁶⁰*Id.*

⁶¹*Id.*

7. *Law Enforcement Access*

Law enforcement agencies are also turning to voice assistant data in criminal investigations.⁶² In one of the first known cases, police requested recordings from an Amazon Echo device as part of a murder investigation in 2015.⁶³ This case set a precedent for using voice assistant data in legal contexts, leading to concerns about governmental surveillance and the erosion of privacy in homes equipped with always-on devices.⁶⁴ Such instances suggest a growing trend in which voice assistant data may be accessed without adequate safeguards for user privacy.

Legal Framework

In today's digital age, voice assistants (VAs) have seamlessly integrated into daily life, collecting extensive data—from search histories and personal preferences to highly sensitive biometric information such as voiceprints.⁶⁵ This data's sheer volume and sensitivity underscore the critical need for robust protections to prevent exploitation and misuse. In the European Union, the **General Data Protection Regulation (GDPR)** has set a comprehensive standard for safeguarding personal data, granting individuals substantial rights over how their information is collected, processed, and stored. Similarly, India has recently introduced the **Digital Personal Data Protection (DPDP) Act, 2023**, which seeks to regulate data privacy and protection in an increasingly interconnected world. Given the widespread use of voice assistants, it is essential to explore how effectively the DPDP Act addresses the specific challenges posed by these technologies and to what extent it aligns with the stringent protections offered by the GDPR.

Data Collection and Processing under the DPDP Act

The DPDP Act emphasises the need for **explicit consent** for collecting and processing personal data.⁶⁶ Voice assistants must inform users (Data Principals) about the nature of the data being collected and the purpose for which it will be processed, ensuring compliance with the principle of **informed consent**.⁶⁷ For instance, when a voice assistant collects data to personalise

⁶² D. Cox, *supra* note 29.

⁶³ Elliott C. McLaughlin, *Suspect OKs Amazon to Hand over Echo Recordings in Murder Case* | CNN Business, CNN (2017), <https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html> (last visited Oct 19, 2024).

⁶⁴ *Id.*

⁶⁵ Divya Pinheiro et al., *Making Voices Heard Literature Surveys: Voice Interfaces and Privacy*, THE CENTER FOR INTERNET AND SOCIETY.

⁶⁶ Digital Personal Data Protection Act, 2023, Section 6.

⁶⁷ Digital Personal Data Protection Act, 2023, Section 5.

responses or provide recommendations, it must notify the user and obtain consent specifically for that purpose. The Act mandates that consent must be free, informed, specific, and unambiguous.⁶⁸ Importantly, Data Principals have the right to withdraw their consent at any time, and this process must be as simple as giving consent.⁶⁹ This aligns with the Act's principle of user autonomy, allowing users to control their data at all times.

In terms of **data retention**, the DPDP Act stresses data minimisation, stipulating that personal data should only be retained for the period necessary to fulfill the stated purpose (Section 8). For voice assistants, this would mean that once a particular command or request has been processed, the voice recordings or related data should not be stored indefinitely. The obligation to delete data after the purpose has been fulfilled ensures that voice assistants do not maintain a repository of unnecessary user data, reducing the risks of data misuse.

User Rights under DPDP and GDPR

The DPDP Act provides several essential rights to Data Principals. Under **Section 11**, users have the **right to access** their data, meaning they can request details on what data has been collected by the voice assistant.⁷⁰ **Section 12** grants users the **right to correction**, allowing them to request the rectification of inaccurate or incomplete personal data held by voice assistants.⁷¹ **Further, it** provides the **right to erasure**, commonly known as the right to be forgotten, which allows users to request that their data be deleted when it is no longer required or if the user withdraws consent.⁷² **Section 13** provides users with the **right to grievance redressal**, ensuring that complaints regarding data handling are addressed by the Data Fiduciary (the entity responsible for processing personal data) before approaching the board.⁷³

The **General Data Protection Regulation (GDPR)**, widely regarded as one of the most comprehensive data protection laws globally, offers similar rights but with additional layers of protection. Under the GDPR, users have the **right to data portability** (Article 20), allowing them to transfer their data from one service provider to another, a right absent in the DPDP Act. Additionally, the GDPR strongly emphasises the **right to restriction of**

⁶⁸ Section 6, *supra* note 66.

⁶⁹ Digital Personal Data Protection Act, 2023, Section 6(4).

⁷⁰ Digital Personal Data Protection Act, 2023, Section 11.

⁷¹ Digital Personal Data Protection Act, 2023, Section 12.

⁷² *Id.*

⁷³ Digital Personal Data Protection Act, 2023, Section 13.

processing (Article 18), which enables users to limit the processing of their data in certain circumstances, further empowering individuals over how their personal data is being used.

Moreover, GDPR provides robust safeguards against **automated decision-making** and **profiling** that may have legal or significant effects on individuals without human intervention.⁷⁴ This is highly relevant for voice assistants, which often rely on machine learning algorithms to profile users based on their voice commands, preferences, and interaction patterns. The GDPR ensures that individuals have the right to request human intervention in such decisions, challenge the decision, or obtain an explanation for the logic involved. The DPDP Act, however, does not explicitly address protections against automated profiling. By incorporating similar provisions, the DPDP Act could safeguard users from the potential risks of being subjected to decisions made solely through automated processes, particularly in targeted advertising and service personalisation.

Data Fiduciary Obligations and Comparisons with GDPR

The DPDP Act imposes several obligations on Data Fiduciaries, the entities responsible for collecting and processing personal data.⁷⁵ They must ensure that data processing is conducted lawfully, fairly, and transparently, which includes implementing appropriate security safeguards to protect against data breaches.⁷⁶ Voice assistant providers must also comply with data retention limits and ensure that personal data is not processed beyond the specified purpose. In case of a **data breach**, Section 8(6) of the DPDP Act mandates that the affected Data Principals and the Data Protection Board be notified, ensuring transparency and accountability.

In comparison, the GDPR imposes stricter accountability measures on Data Controllers (equivalent to Data Fiduciaries under DPDP). For instance, under GDPR, entities must conduct **Data Protection Impact Assessments (DPIAs)** when processing personal data that poses high risks to individuals' rights (Article 35). This provision is notably absent in the DPDP Act, which could be a critical area for improvement, particularly as voice assistants handle sensitive biometric data like voice patterns.

⁷⁴ Regulation (EU) 2016/679, art. 22, 2016, Official Journal of the European Union, (L 119) 46.

⁷⁵ Digital Personal Data Protection Act, 2023, Section 8 & 10.

⁷⁶ Digital Personal Data Protection Act, 2023, Section 8.

Another notable difference is the **Data Protection Officer (DPO)** requirement under GDPR. Organisations must appoint a DPO if they engage in large-scale processing of personal data, especially sensitive categories.⁷⁷ The DPDP Act has introduced the concept of **Significant Data Fiduciaries**, which are subject to additional requirements, including appointing a DPO.⁷⁸ However, this provision is limited to entities above a certain threshold, potentially excluding smaller voice assistant services that still process sensitive data at significant volumes.

Children's Data Protection: GDPR vs DPDP

The GDPR and the DPDP Act acknowledge the need to protect children's data but differ in their approaches. The GDPR sets the age of consent for data processing at 16 years (allowing member states to lower it to 13) and requires parental consent for minors below this age.⁷⁹ It also mandates that information provided to children must be clear and understandable, ensuring transparency in data usage. In contrast, the DPDP Act establishes a higher age threshold of 18 years for consent, requiring parental approval for processing children's data.⁸⁰ However, more detailed provisions are needed to ensure that children and their guardians fully comprehend how their data is used. The GDPR's focus on presenting data policies in a child-friendly manner serves as a critical safeguard that could significantly enhance the DPDP Act, especially given the rising use of voice assistants among younger audiences.

Improving DPDP with Insights from GDPR

The DPDP Act can be strengthened by adopting several features from the GDPR, in addition to those mentioned earlier. Firstly, incorporating provisions for **Data Protection by Design and Default**, as mandated under GDPR (Article 25), would ensure that privacy is integrated into the development of voice assistant technologies from the outset, minimising data risks. This principle mandates that companies proactively incorporate privacy safeguards during the design stages of their systems rather than retrofitting protections after deployment.⁸¹

⁷⁷ Regulation (EU) 2016/679, art. 37 & 38, 2016, Official Journal of the European Union, (L 119) 55.

⁷⁸ Digital Personal Data Protection Act, 2023, Section 10.

⁷⁹ Regulation (EU) 2016/679, art. 8, 2016, Official Journal of the European Union, (L 119) 37.

⁸⁰ Digital Personal Data Protection Act, 2023, Section 2(f) & 9.

⁸¹ Regulation (EU) 2016/679, art. 25, 2016, Official Journal of the European Union, (L 119) 48.

Secondly, The **GDPR** provides robust protection for **biometric data**,⁸² categorising it as a special category of sensitive personal data under **Article 9**. The regulation prohibits processing biometric data, including voiceprints used by voice assistants (VAs), unless specific conditions such as **explicit consent** or legal necessity are met. This heightened level of protection ensures that biometric data is handled with the strictest safeguards, requiring organisations to justify and secure the data they collect. In contrast, the **DPDP Act of 2023** does not explicitly classify biometric data as a separate sensitive category, instead addressing it under broader personal and sensitive data regulations. While the DPDP Act mandates obtaining consent for data processing and offers general protections for sensitive data, the lack of explicit mention of biometric data means it lacks the same rigour as GDPR in safeguarding such inherently personal information. Given the growing reliance on VAs and other biometric-dependent technologies, this represents a gap in DPDP's framework, which could benefit from adopting GDPR's stringent approach to biometric data protection.

Thirdly, **guidelines issued by the European Data Protection Board (EDPB)** under GDPR offer valuable insights into the practical application of data protection principles. For instance, the **EDPB's Guidelines 02/2021 on Virtual Voice Assistants** provide detailed recommendations on how voice assistants should handle consent, data minimisation, transparency, etc. Adopting a similar mechanism within the DPDP framework, where a dedicated Data Protection Authority periodically issues specific guidelines, would allow the Indian framework to remain responsive to evolving technologies and emerging data protection challenges.

Finally, The GDPR's emphasis on **data portability**⁸³ and protection against automated decision-making⁸⁴ could also be valuable additions to the DPDP Act. Given the growing use of AI in personalising voice assistants, enabling users to transfer their data across platforms and protect them from potentially harmful automated decisions would offer greater control and transparency.

⁸² Regulation (EU) 2016/679, art. 4(14), 2016, Official Journal of the European Union, (L 119) 34.

⁸³ Regulation (EU) 2016/679, art. 20, 2016, Official Journal of the European Union, (L 119) 45.

⁸⁴ Regulation (EU) 2016/679, art. 22, 2016, Official Journal of the European Union, (L 119) 46.

Conclusion

The rapid proliferation of voice assistants (VAs) has transformed the landscape of human-computer interaction, bringing unprecedented convenience and significant data security challenges. As these technologies gather vast amounts of personal data—including sensitive information such as voiceprints and user preferences—ensuring robust protections becomes imperative. This research paper has examined the regulatory frameworks established by the **General Data Protection Regulation (GDPR)** in the European Union and the **Digital Personal Data Protection (DPDP) Act of 2023** in India, highlighting their approaches to safeguarding various aspects of personal data security.

As voice assistants become increasingly embedded in daily life, the potential to misuse sensitive personal data underscores the urgent need for adaptive and comprehensive legal frameworks. By integrating essential provisions from the GDPR, such as enhanced biometric data protections, clearer guidelines for children's data, etc. the DPDP Act can strengthen its effectiveness in protecting personal data in the digital age. Ultimately, a proactive approach to data protection will ensure that the benefits of voice assistants can be harnessed while minimising the risks associated with data privacy and security.