LEGAL LOCK JOURNAL

2583-0384

VOLUME 4 || ISSUE 2

2024

CONSUMER DATA PRIVACY IN DIGITAL MARKETING: A CRITICAL ANALYSIS OF LEGAL REGULATIONS

Tarinee Pradip Siddhaye[1]

ABSTRACT

India is a country with 75.9 crores of internet users. By 2025, it is set to reach 90 crores. India ranks 10th globally in data breach and online privacy violations incidents in 2023. In the world of digital marketing, a world heavily reliant on customer data, it is beneficial to provide a more targeted, personalized experience to a customer. But at the cost of selling customer's data to advertisement agencies. The study shed light on understanding the gap between policy and implementation of policy. How many times have you encountered a situation where an advertisement for a beauty product or electronic gadget appeared on your social media feed while you were having a real-time conversation about a similar product? Here, consumer's sensitive data is used for online frauds and scams. Online cookies are everywhere that collect names, home addresses, credit card numbers, and GPS coordinates to complete the transaction. In the e-commerce market, Consumers expect confidentially of their data and transparency in the Privacy Policy. Consumer privacy protection comes under the ambit of The Consumer Protection Act, 2019 which overlaps with the Information Technology Act, 2000 as well as The Digital Personal Data Protection Act, 2023. The research suggests issuing guidelines to prevent unauthorised disclosure of personal information by consent and opt-out mechanisms, the removal of third-party cookies, adopting a privacy-by-default approach, and translating the typical legal language in a privacy policy into something more digestible that builds a strong relationship with their consumers. Also, vendors and intermediaries should respect the privacy principles. Consumer awareness about the safe use of electronic commerce should be promoted by Government, businesses, and consumer groups. Therefore, the balance of customer privacy and data-driven marketing is key.

KEYWORDS: *consumer protection, privacy, data, digital marketing, advertisement*

[1]The author is a student at KES' Shri Jayantilal H. Patel Law College

INTRODUCTION

Have you ever wondered how your search related to a specific product on a search engine pops on social media or other websites as an advertisement? The answer is the time a user installs any application or enters a website asks for a mandatory "cookie" acceptance, required to enable core site functionality allows Universal Analytics to analyse site usage so they can measure and improve performance which in some cases can prove to be a privacy concern. The consumer's digital footprint with personal data[2] including name, sex, address, email ID, contact number, contact list, location, credit card details, likes, dislikes etc. extracted under the name of providing personalised services or even sold to the third parties without the consent of the customer.

India is the second largest online ecosystem in the world with over 75.9 crores of active internet users, with the rising internet penetration, this number is bound to increase sharply in the next 5 years.[3] In this technological era, digital advertising is commonly defined as the practice of delivering promotional content to users through various online and digital channels by leveraging mediums such as search engines, mobile apps, social media, email, and affiliate programs.[4] A classic example of data manipulation is airline flight ticket prices.

As technology advances, so do the advertisements[5] consumers receive. In 2018, in the case of **the Facebook-Cambridge Analytica Leak**, Cambridge Analytica used the personal data of 8.7 crore Facebook users to create psychological profiles of voters for Trump's political campaigns.[6] Whereas in 2020, data of over 100 crore customers of Amazon, Flipkart, Jiomart and Airtel were sold on the dark web for $6,000.[7] One's data is currency to the other hence, 'nothing is for free'.

---

[2] The Digital Personal Data Protection Act, 2023, sec.2 (t).

[3] Pti. (2023, May 4). *Over 50% Indians are active internet users now; base to reach 900 million by 2025: report*. The Hindu. https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece

[4] *What is Digital Advertising? The Future of Digital Advertising*. (2021, December 16). Spiceworks. https://www.spiceworks.com/marketing/advertising/articles/digital-advertising-primer-martech-101-2/

[5] The Consumer Protection Act, 2019, sec. 2(1).

[6] Webdeveloper. (n.d.). *Facebook–Cambridge Analytica Data Scandal|Business Ethics|Case Study|Case Studies*. ICMR. https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/BECG160.htm

[7] Chandrashekhar, A. M. a. A. (2021, January 6). Juspay Data Leak fallout: RBI swings into action to curb cyberattacks. *The Economic Times*. https://pushstg.indiatimes.com/tech/technology/juspay-data-leak-fallout-rbi-swings-into-action-to-curb-cyberattacks/articleshow/80125430.cms

DEFINITIONS

1. **Consumer** means a person who buys or avails of goods or services online or through electronic means.[8]
2. **Advertisement** refers to any audio or visual publicity, representation, endorsement, or pronouncement made using, inter-alia, electronic media, internet, or website.[9]
3. **The data principal** is the person to whom the personal data relates.[10]
4. **Data fiduciaries** deal with the processing of personal data.[11]

PRIVACY CONSIDERATIONS

The term privacy is not defined under any act or statute and a right without definition could be a right without protection. But it can be described as "the right to be let alone". Data privacy is one branch of data management that deals with handling personal data by following data protection laws, and regulations. In the landmark case of ***Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.***[12] also known as the Aadhaar case, the Supreme Court recognised the right to privacy as a part of the right to life and personal liberty. The right to privacy is the fundamental right provided under **Article 21**[13] of the Constitution of India of 1950 and **Article 12**[14] of the Universal Declaration of Human Rights of 1948.

The following are the consumer privacy features offered by government agencies:

- Do-not-call lists.
- Verification of transactions by email or telephone.
- Technologies for email.
- Passwords and multifactor authentication.
- Encryption and decryption of electronically transmitted data.

[8] The Consumer Protection Act, 2019, sec. 2 (7).
[9] The Consumer Protection Act, 2019, sec. 2 (1).
[10] The Digital Personal Data Protection Act, 2023, sec. 2 (j).
[11] The Digital Personal Data Protection Act, 2023, sec. 2 (i).
[12] AIR 2017 SC 4161.
[13] No person shall be deprived of his life or personal liberty except according to procedure established by law.
[14] No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

- Opt-out provisions in user agreements for bank accounts, utilities, credit cards and other similar services.
- Digital signatures and biometric identification technology.

PRIVACY *v.* RIGHT TO INFORMATION

The Digital Personal Data Protection Act (DPDPA) 2023 amended **the Right to Information Act of 2005** leading to personal data never being disclosed as part of a right to information request.

REGULATORY LANDSCAPE

At present 137 out of 194 countries have legislation to secure the protection of data and privacy of the data principal.[15] **The Ministry of Information and Broadcasting** and **the Advertising Standards Council of India (ASCI)** are bodies that regulate digital advertising along with the following acts:

- **The Information Technology Act of 2000** includes provisions related to data disclosure and the failure to protect data. **Section 79** provides liability of content providers in digital advertising falls under the definition of intermediary. After the Information Technology (Amendment) Act of 2008, a section related to privacy was added namely **Section 43A** that stipulates if any corporate body is negligent in maintaining reasonable security practices, resulting in wrongful loss or gain to any person, then he/she is liable to compensate the affected party. Although after The Digital Personal Data Protection Act (DPDPA) 2023 will come into force said section shall be omitted. Moreover, the Ministry of Electronics and Information Technology (MEITY) Rajeev Chandrasekhar announced that the Digital India Act 2023 going to replace the present act.[16]
- Subsequently, in June 2011, India passed **Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules,**

[15] *Data protection and privacy legislation worldwide*. (n.d.). UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide#:~:text=137%20out%20of%20194%20countries,in%20only%2048%20per%20cent.

[16] Oke, Y. (2023, August 8). *Explained: The Digital India Act 2023*. Vidhi Centre for Legal Policy. https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/#:~:text=Rajeev%20Chandrasekhar%2C%20the%20Minister%20of,%2C%20a%20future%2Dready%20legislation.

2011,[17] subordinate legislation that included various new rules that apply to companies and consumers, mandates prior written consent from the data subjects for publishing or sharing personal information to the third party.

- **The Consumer Protection Act, 2019** explicitly includes e-commerce transactions within its scope, defining e-commerce as the buying or selling of goods or services including digital products over digital or electronic networks by strengthening consumer protection from online transactions. It aims to protect the interests of the consumers defined under **Section 2(7)** and **establish the Central Consumer Protection Authority (CCPA)** under **Section 10** to settle disputes of consumers including false or misleading advertisements that are prejudicial to the interests of the public and consumers as a class. The rights of consumers are defined under **Section 2(9)**. Further unfair trade practice **Section 2(47)** includes unauthorised disclosure of personal information.

- While, **the Consumer Protection (E-commerce) Rules, 2020** under the provisions of the Consumer Protection Act enacted to safeguard consumers from unfair trade practices in e-commerce outline the responsibilities of e-commerce entities as well as specify the liabilities of marketplace and provisions for customer grievance redressal. The Department of Consumer Affairs observed that dark patterns are a subset of unfair trade practices that involve using patterns to deceive, coerce, or influence consumers into making choices that are not in their best interest. The rules apply to OTT platforms and online service platforms such as those offering education, booking transportation, etc. The rules contain provisions for compliance, manipulations, controlling market structure, grievance redressal, and penalties.

- **The Digital Personal Data Protection Act (DPDPA) 2023** aims to protect personal data, uphold privacy, promote fairness and transparency, and safeguard individual rights. It is the primary data protection law in India that governs how entities process users' personal data and applies to the processing of "personal data" either

(i) Within India; or

(ii) Outside of India.[18]

[17] MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY. (2011). Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. In *THE GAZETTE OF INDIA: EXTRAORDINARY*. https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[18] The Digital Personal Data Protection Act, 2023, sec. 16.

in connection with offering goods or services to Data Principals within the territory. The Act will make it mandatory for entities collecting user data to process the data only after obtaining express user consent, with some exceptions. **The Data Protection Board of India** is to be an independent regulatory body. **Section 17(2)(a)** provides a blanket exemption to Law enforcement agencies, government agencies, banks, and a few financial institutions from data privacy laws for data processing. Further in **Section 17(3)**, limited exemptions are provided to the startups. All organisations must appoint a Data protection officer, and independent data auditor, who help the businesses comply with the law. The act prescribes a penalty of fee of up to Rs. 250 crores for offences related to:

(a) Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under **Section 8(5).**

(b) Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under **Section 8(6)**.

SCOPE OF CCPA AND DPB

It appears that both the Central Consumer Protection Authority (CCPA) and the Data Protection Board of India will have jurisdiction to inquire into the unauthorised disclosure of personal data of the consumer/user by overlapping between data protection and cyber security. However, the DPDP Act has a broader scope because of its definition of a 'data principal' compared to the definition of 'consumer' under the CPA. The CCPA can pass an order for the discontinuation of unfair practices with an option of seeking compensation by approaching the appropriate consumer redressal commission.[19] Whereas, the DPB has only the power to issue directions and impose penalties and no compensation to the aggrieved party.

APPLICABILITY OF THE EUROPEAN UNION'S (EU'S) GENERAL DATA PROTECTION REGULATION (GDPR)

General Data Protection Regulation is not directly applicable to the Indian citizens but if the data is related to European citizens and the company is an Indian company based in India, GDPR is applicable for that company. Even The Digital Personal Data Protection Act of 2023 align with this regulation.

[19] The Consumer Protection Act, 2019, sec. 20.

CONCLUSION

The use of the internet increased after the 2000s because of the introduction of social media platforms to connect people and data became the most valuable asset on earth in this digital era. Websites require data and statics to run their business but at the cost of consumer's privacy. Data collected are not properly regulated resulting in misuse of it. In several incidences, the Supreme Court clarified the importance of the right to privacy. The hypothesis of this research paper "Customer's digital privacy is a paramount responsibility" **is hence proved.**

Individual activities are constantly tracked to make a blueprint of how consumers think and what are their interests. The Consumer Protection Act of 2019 with the aid of The Digital Personal Data Protection Act of 2023 protects the interests of the victims of data breaches. The Central Consumer Protection Authority and the Data Protection Board of India have their separate jurisdiction which regulates digital marketing and personal data of the consumer. It is hoped that The Digital Personal Data Protection Act of 2023 will soon come into force to limit unauthorised uses of the personal data of the consumer. Hence, effective legislation and effective implementation of its provisions are very necessary to bridge the gap between what is on paper and what is in reality. As Gary Kovacs once stated,

"*Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.*"

SUGGESTIONS

Based on the analysis of the secondary data collection, the following suggestions can be recommended for the issue of customer privacy:

- The government should run workshops related to awareness of the rights of the consumer.
- The online grievances redressal mechanism with the feature of tracking its status of progress should be implemented.
- Customer-first approach should be adopted by the organisation.
- The Organisations should provide information in plain language about the handling of customers' personal information.
- The personal data should be used only after the voluntary consent of the user.

- Privacy policies should be transparent and compulsory acceptance of mandatory cookies should be regulated.
- The consumer should be aware of opt-out and opt-in options by the organisation.
- The right to disposal should be given to the data principal to request the deletion of information when he/she withdraws consent.
- Organisations should share information related to where that data is stored and for how long.
- No business for whatsoever reason, tracks, or collects the behavioural analytics of children for targeted advertising.