Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

A Comprehensive Study on AI Assurance of Data Privacy with Common Operational Governance: Build A Consumer Trust in Digital Marketing

Dr.B. Jagadeeswaran[1], V. Jenifer[2], Dr.V. Devi[3]

[1]Associate Professor & Head, PG & Research Department of Commerce, Thiruthangal Nadar College, Selavayal, Chennai -51
[2]Ph.D Full Time Research Scholar, PG & Research Department of Commerce, Thiruthangal Nadar College, Selavayal, Chennai – 51.)
[3]Principal, Thiruthangal Nadar College, Selavayal, Chennai – 51.

ABSTRACT
The rapid proliferation of Artificial Intelligence (AI) across various sectors necessitates robust frameworks for AI assurance, data privacy, and common governance to maintain consumer trust. This paper explores the critical need for AI assurance frameworks to safeguard data privacy within the dynamic landscape of digital marketing, addressing the ethical challenges and managerial implications arising from AI's pervasive influence on consumer data.Ethical AI in digital marketing demands more than compliance with legal standards it requires a proactive commitment to transparency, fairness, user autonomy, and accountability. This paper explores the intersection of AI ethics, data privacy, and responsible digital marketing governance, emphasizing the need for to build consumer trust in digital marketplace. This study measures Ethical AI, requires moving beyond mere compliance to proactively address algorithmic fairness and transparency. Data Privacy protocols must be foundational, predicated on the principles of data minimization, purpose limitation, and privacy-by-design empowerment. at last, effective Responsible Digital Marketing Governance provides the structured framework and ethical standards.

Keywords: Data privacy, Ethical AI, Governance, Responsible AI.

1. INTRODUCTION

With progression of artificial intelligence (AI) and its addendum in digital marketing, digital business has progressed leaps and bounds. In this new era of modernization, the digital marketers can gather data of customers about their choices and preferences. This huge amount of data then can be analysed using AI and based on this data AI can predict consumer behaviour and it can generate targeted campaigns which in return, helps the digital marketers in achieving the desired results (Pazzanese, 2020). The AI has immense potential in digital marketing however the use of AI in digital marketing raises certain ethical concerns like privacy of customer's data, consent of customer's before gathering their data, un-bias in algorithms, transparency of the process. If the digital business who are using IA are made accountable, then only it will build consumers' trust in the process.

Unlike humans the AI can process huge amount of data to recognize patterns, make decisions and judge like humans do. (Verma, Sharma, Deb, Maitra, 2021). In 2023, the Government of India took cognizance of the rapidly evolving AI landscape in the country and committed to a proportional, future-focused, and adaptive governance framework to respond to its dynamic needs that should enforce compliance and ensure effective governance. (India AI Governance Guidelines: Empowering Ethical and Responsible AI, n.d).

India's newly drafted AI Governance Guidelines are now being launched in the public domain with a dual purpose: to maximise the developmental and economic gains from AI by fostering innovation and adoption at scale, and to mitigate associated risks in a manner that safeguards individuals, protects societal interests, and upholds democratic values. At last, that guidelines provide a framework for the development and deployment of safe, trustworthy, responsible, inclusive and accountable AI systems, such that cutting-edge AI can be harnessed in concert with other transformative technologies to anchor the long-term growth, resilience and sustainability of India's digital ecosystem. (India AI Governance Guidelines: Empowering Ethical and Responsible AI, n.d).

Some Key Differences are:

Aspect	AI Regulations	AI Ethics
Purpose	Legal compliance and governance	Moral and responsible AI use
Scope	Laws, policies, and guidelines	Principles and best practices
Enforcement	Government and regulatory bodies	Businesses and ethical AI advocates
Examples	GDPR, CCPA, AI Act (EU)	Bias mitigation, transparency, fair AI usage

ETHICAL AI

Ethical AI refers to the practices and principles used to ensure that artificial intelligence systems are developed and operated in a manner that aligns with ethical standards. This includes delivering benefits to society while minimizing harm**.**Ethical AI encompasses methods and practices that ensure AI technologies act in accordance with human values, such as fairness, transparency, accountability, and privacy, while managing risks of bias, discrimination, or harm to individuals and society. These principles guide organizations toward responsible AI practices that support trust and long-term viability in both business and society. Organizations that practice ethical AI implement clear policies, review processes, and continuous assessment to ensure their systems remain aligned with human rights, safety, and inclusivity. AI ethics refers to a framework of moral principles and guidelines that govern the development and applications of artificial intelligence.

Why ethical AI matters? Ethics is a set of moral principles or concepts of moral that guide behaviour – what is right or wrong. Where ethical describes something that follows moral principles or which is morally right.Ethics of AI is Principles of developing AI to interact with other AIs ethically. Without an ethical approach, AI can cause harm - such as perpetuating bias, violating privacy, and undermining trust. Ethical AI ensures systems are safer, fairer, and more accountable, all of which are critical for public adoption and regulatory compliance.

2. Key ethical considerations in AI include:

Data privacy: The need for robust protections that ensure user data is secure and not exploited.
Fairness: Ensuring algorithms treat individuals equitably, avoiding discrimination.
Transparency: Providing clarity about how AI systems arrive at decisions, enabling accountability.
Accountability: Establishing clear lines of responsibility for the outcomes produced by AI systems.
Social and cultural impacts: Recognizing how AI affects cultural norms and social structures.

Key Steps for Ethical AI Implementation:

1. Assess AI Readiness: Evaluate existing AI tools and their alignment with ethical guidelines.
2. Train Teams on AI Ethics: Educate employees on ethical AI principles and responsible data handling.
3. Develop AI Governance Policies: Define company-wide policies for AI use, data privacy, and to be neutral.
4. Integrate AI Ethics Audits: Conduct periodic audits to ensure compliance with ethical and legal standards.
5. Engage with Ethical AI Communities: Collaborate with AI ethics experts, regulatory bodies, and industry leaders to stay informed on best practices.

Implementing ethical AI in marketing requires a proactive approach to fairness, transparency, and consumer trust. Businesses must prioritise data privacy, bias mitigation, and responsible AI deployment. Regular audits, user consent mechanisms, and inclusive AI training help ensure compliance and ethical integrity.

Ethical AI in digital marketing is not just a compliance necessity - it is a competitive advantage. By prioritising transparency, fairness, and data protection, businesses can harness AI's potential while maintaining consumer trust and regulatory compliance.

3. DATA PRIVACY AND RESPONSIBLE DIGITAL MARKETING GOVERNANCE

DATA PRIVACY:

One of the most over-riding and prevalent issues surrounding today's digital society is privacy. In the digital age, privacy covers various aspects, such as information privacy, communication privacy, and individual privacy, and each of these aspects is unique in its own right. Information privacy concerns the protection of personal data collected and stored by entities. Communication privacy on the other hand addresses the unauthorized use and distribution of personal communications. Individual privacy pertains to the protection of one's identity within online.

It is essential to understand that privacy is not just about hiding one's affairs from the public eye; it's about having the control and freedom to choose what information about oneself can be shared and who has the access to it. Understanding privacy in the digital age also means recognizing its economic value. Personal information is a valuable asset for many businesses because it allows them to cater to their customers more effectively. However, the unauthorized and unregulated use of such information can lead to a multitude of problems for individuals, including identity theft, financial fraud, and indiscriminate surveillance. Governments have their reasons for collecting data, often related to issues such as national security and crime prevention. However, without proper oversight and regulation, such collection can lead to an infringement on civil liberties. Data privacy refers protection of personal data to ensure that individual's information is collected, stored, and used responsibly, ethically and in compliance with legal regulations. It involves safeguarding sensitive data from unauthorised access, granting individuals the right to understand how their data is used, and empowering them to make informed choices regarding its utilization. (Priya & Amity Institute of Information Technology, 2024). Security measures are crucial for protecting data from unauthorized access, breaches, and other risks like financial loss and reputational damages.Use encryption to secure data during transmission and storage, implementing access controls to restrict data access to authorized personnel and conduct regular security assessment. Data privacy protects individual's personal information, maintains trust, ensures compliance with data protection laws, and it foundational for ethical data use in the digital age.

To ensure proper management of personal data, key essentials are, data encryption, access control, legal and regulatory compliance, data minimization and purpose limitation (collect only necessary data), transparency and consent, regular auditing and monitoring, ethical data practices, accountability. To improve personal data privacy individuals also can take several practical steps to safeguard their information like use strong, unique passwords, enable Two-Factor Authentication (2FA) which requires a second verification step such as a code sent to your phone, limit sharing of personal information, review privacy settings, use secure and Encrypted connections, be vigilant against phishing and scams, limit cookies and trackers, controls App permissions. By implementing these steps individuals can enhance control over their personal information and significantly reduce the risk of data breaches or misuse.

RESPONSIBLE DIGITAL MARKETING GOVERNANCE:

Responsible Digital Marketing Governance refers to the structured framework and practices that organizations implement to direct control and oversee their digital marketing activities ethically, efficiently and compliantly. It ensures that digital marketing efforts align with business goals while upholding transparent accountability, data privacy, legal regulations and ethical standards. Modern data privacy encompasses not only traditional personally identifiable information (PII) but also behavioral data obtained through AI, requiring comprehensive protections across multiple systems and jurisdictions. Laws and regulations play an essential role in addressing digital privacy concerns.

Some key aspects are,

1. Clear roles and responsibilities within the digital marketing team.
2. Established policies and procedures for content creation, data handling, and campaign [Effort designed to promote a product service or brand to a target audience] approvals.

3. Continuous monitoring and measurement of campaign performance and compliance [Businesses (organizations that operate commercially to promote product or services online) adhering to laws, regulations and guidelines that govern how personal data is collected, processed, stored and used].
4. Emphasis on data privacy and adherence to regulations like GDPR, CCPA, CAN-SPAM and sector specific rules.

COMMON REGULATIONS ADHERING IN COUNTRIES

GDPR: GENERAL DATA PROTECTION REGULATION

It is a strict data protection law enacted by the European union to offer individuals more control and transparency over their personal data. Obtained informed consent from users before collecting or using the personal data of EU residents. Consent must be freely given, specific and revocable. Informed consent - before processing personal data, provide clear privacy policies, allow individuals rights to access, delete their data and ensure data security.

Secure data by using encryption, access controls and regular audits to prevent unauthorized access, leaks or breaches. If personal data is transferred across countries, marketers must ensure those countries offer adequate protection using legal mechanisms where necessary.

CCPA: THE CALIFORNIA CONSUMER PRIVACY ACT

It is a state law designed to enhance privacy rights and consumer protection for residents of California. Consumers have the right to know what personal data is collected, used, shared or sold. They can opt-out of the sale of their data through a clear “Do not sell my personal information” link. Consumers can request access to their personal information and request deletion of it. Companies must update their privacy policies annually to include CCPA rights.

Thus, CCPA helps empower consumers with privacy right and holds businesses accountable for responsible data handling. Unlike GDPR, CCPA emphasizes notice and consumer control without mandatory consent in many cases but demands clear opt-out mechanisms and privacy disclosures.

CASL: THE CANADIAN ANTI-SPAM LEGISLATION

Is one of the world’s strictest laws designed to regulate commercial electronic messages (CEMs) such as emails, SMS, Social media messages, and instant messages with a commercial purpose. It aims is to protect Canadians form spam, electronic threats like phishing and malware, and ensure a secure and trustworthy online environment. Requiring consent (either express or implied) before sending commercial electronic messages. Consent must be documented and can be withdrawn by recipients at any time.CASL also prohibits the installation of computer programs without consent and the alteration of transmission data. It excludes messages necessary for business relationships or certain non-commercial communications. Overall, CASL promotes responsible electronic marketing by ensuring transparency, consent and consumer choice with strict penalties to discourage spam and protect privacy.

CAN-SPAM ACT: CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPTHY AND MARKETING ACT

It is a U.S law that regulates commercial email messages to protect consumers from deceptive and unwanted emails. It applies to all businesses sending commercial emails to U.S recipients and sets rules to ensure responsible email marketing. This act doesn’t require prior consent before sending emails, it

mandates a clear, easy way for subscribers to opt-out and prohibits selling or transferring email addresses of those who have opted out Non-compliance may result in enforcement actions and fines.

Key requirements are:

1. Use accurate and truthful sender information in headers and subject lines.
2. Clearly identify the email as an advertisement.
3. Include a valid physical postal address of the sender.
4. Provide a simple, visible way for recipients to opt-out (unsubscribe) from future emails.
5. Honor opt-out requests promptly within 10 business days.
6. Maintain the opt-out mechanism active for at least 30 days after sending the email.
7. Do not use deceptive subject lines or false header information.
8. Monitor third parties sending emails on your behalf to ensure compliance.

Overall, the CAN-SPAM ACT promotes transparency, consumer choice, accountability in email marketing, helping businesses build trust while reducing spam and fraud. This makes CAN-SPAM compliance an essential part of responsible digital marketing.

In India, key regulations protecting individual data in digital marketing includes:

DIGITAL PERSONAL DATA PROTECTION ACT 2023 (DPDP ACT)

This is the foundational law for data privacy in India, governing the collection, processing, and storage of personal data. It mandates lawful purpose, consent – based processing, transparency, data subject rights like access, correction and deletion and rules for cross – border data transfers. It also establishes a Data Protection Board for enforcement and penalties up to Rs.250 crores for non-compliance. DPDP act and rules apply to Indian organizations as well as foreign entities collecting or processing data of Indian residents, thus covering digital marketing activities extensively.

DIGITAL PERSONAL DATA PROTECTION RULES, 2025

These rules operationalize the DPDP Act and provide detailed guidelines on responsibilities of data fiduciaries (organizations controlling data) and data processors. They specify consent requirements, breach notification protocols, and transparency standards in clear language.

INFORMATION TECHNOLOGY ACT, 2000 AND IT (Reasonable security Practices) RULES

It is India's primary legislation governing digital transactions, cybercrimes, electronic records, and the responsibilities of digital intermediaries. It provides the legal framework for the recognition of electronic contracts, digital signatures and sets out specific offences and penalties for cybercrime. These laws address cybercrime, protection of sensitive personal data and guidelines for securing corporate data systems. The IT Act 2000 and related rules establish accountability for cyber activities, protect individual privacy and balance user rights and government regulation in India's digital ecosystem. They offer remedies for victims of cybercrime and clarify the legal responsibilities of intermediaries and digital platforms.

Important sections and IT rules:

Section 65-74: cover a range of offences such as tampering with computer documents, hacking, identity theft, cheating via computer, cyber terrorism with punishments ranging from fines to life imprisonment.

Section 69A: Empowers the government to block public access to information if it threatens national security, public order or foreign relations.

Section 79: Establishes "safe harbour" for intermediaries (like social media), exempting them form liability for user-generated content unless they fail to act on government notifications about unlawful content.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules ,2021: Specify due diligence requirements for platforms, including removing unlawful information upon receiving actual knowledge.

Related Amendments: The Act was amended in 2008 to address new offences, powers of state to intercept data and penalties. Later, related statutes like the Digital Personal Data Protection Act, 2022, further strengthened privacy protection.

SECTOR – SPECIFIC REGULATIONS

Sector – specific regulatory requirements are vary depending on the industry in which a business operates. These rules are designed to address unique privacy, advertising and communication concerns relevant to different sectors. Practically, sector – specific rules compel marketers to tailor their consent mechanisms, messaging content, data management, and privacy policies according to the applicable legal framework for their industry and location, ensuring responsible and lawful marketing practices. sector – specific rules are customized compliance requirements that digital marketers must follow depending on the regulatory environment impacting their industry.

Some aspects are:

RBI (Reserve Bank of India) guidelines for banking and payment data security.

IRDAI (Insurance Regulatory and Development Authority of India) Regulation ruling insurance data protection.

SEBI (Securities and Exchange Board of India) Cybersecurity framework for financial market intermediaries.

CERT-In (Computer Emergency Response Team – India) Detects, responds to, and prevents cyberattacks and data breaches across all government and private sectors. They lead the investigation and containment.

These regulations emphasize explicit consent, transparency, data security, breach reporting, and individual control over personal data, reflecting India's commitment to strengthening data privacy amid rapid digital adoption. In summary, India protects digital marketing data under a robust evolving framework anchored by the DPDP Act, supported by sector – specific rules and cyber laws, mandating responsible data handling and consumer privacy rights.

CONCLUSION

In conclusion, ethical AI is essential for fostering a future where AI benefits humanity without compromising safety, fairness and privacy. Ethical AI is designed to respect human rights, mitigate biases, and promote fairness, transparency, and accountability. While AI ethics focuses on moral and

responsible use, AI regulations are legal frameworks that enforce compliance. Understanding the distinction between these two helps businesses align ethical considerations with regulatory requirements. Effective data privacy practices promote transparency, user control and trust by clearly communicating data collection, usage, sharing and user right. Data privacy is essential for protecting individual right, ensuring transparency and maintaining trust in digital interactions. Ultimately, establish clear governance frameworks with defined roles, responsibilities and accountability to ensure consistent and ethical digital marketing practices. With evolving data protection laws and regulations worldwide, organizations must adopt ethical data governance and proactive security measures to mitigate risks and support a sustainable digital economy.

REFERENCES:

1. Ali, E., Riaz, M., & Rashid, M. (2024). Ethical Considerations in Use of Artificial Intelligence in Digital Marketing. Journal of Peace, Development and Communication,08(02), 340–351. https://doi.org/10.36968/JPDC-V08-I02-25.
2. India AI Governance Guidelines: Empowering Ethical and Responsible AI. (n.d.). IndiaAI.https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai.
3. Siau, K., & Wang, W. (2020). Artificial Intelligence (AI) Ethics. Journal of Database Management, 31(2), 74–87. https://doi.org/10.4018/jdm.2020040105.
4. Understanding Privacy in the Digital Age - IEEE Digital Privacy. (2025, May 13). IEEE Digital Privacy. https://digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age/.
5. Priya, A. & Amity Institute of Information Technology. (2024). DATA PRIVACY AND ETHICS IN THE DIGITAL AGE. In Futuristic Trends in Computing Technologies and Data Sciences (Vols. 3–3, pp. 291–292). https://iipseries.org/assets/docupload/rsl20245027ADD81734B90.pdf.
6. Effectiveness of digital marketing to protect customers through artificial intelligence, 222–226 (2023) https: //doi.org/10.1109/CISES58720.2023.10183618.
7. Artificial intelligence and its ethical implications for marketing. Emerging science journal (2023) https: //doi.org/10.28991/esj-2023-07-02-01.
8. Directory, S. (2025, April 6). Digital Marketing Governance → Term. Climate → Sustainability Directory. https://climate.sustainability-directory.com/term/digital-marketing-governance/.
9. Kumar, V., Rajan, B., Venkatesan, R., &Lecinski, J. (2023). Ethical considerations in AI-based marketing: Balancing profit and consumer trust. The Journal of Joint Park Technology, 44(3), 474. https://doi.org/10.52783/tjjpt.v44.i3.474.
10. Martin, K. D., & Murphy, P. E. (2023). Ethical and legal challenges of AI in marketing: An exploration of solutions. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4396132.
11. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.
12. Aldoseri, B., Al-Khalifa, H. S., & Hamouda, M. (2025). AI ethics: Integrating transparency, fairness, and privacy in AI development. Applied Artificial Intelligence, 39(1), Article 2463722. https://doi.org/10.1080/08839514.2025.2463722.