IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Corruption Of Creation: AI Privacy Breaches, Deepfakes, And The Integrity Of Digital Design

Drishti Agarwal

Student

The Heritage School, Kolkata, India

Abstract

The rapid proliferation of Artificial Intelligence (AI) presents a critical juncture for digital privacy, security, and intellectual property. This review paper systematically analyzes the multifaceted privacy threats inherent in the age of AI, focusing on four core areas: non-consensual data collection practices, the proliferation of deepfakes for misinformation and harm, the contentious use of human creations for AI model training, and the profound impact of data breaches on the integrity of AI-driven product design. Through a synthesis of recent scholarly literature, this paper identifies significant gaps in current legal and ethical safeguards. The findings reveal that opaque data procurement methods, inadequate "opt-out" consent models, and the weaponization of synthetic media pose severe risks to individual autonomy, societal trust, and the foundation of user-centric product development. The paper concludes that a fragmented regulatory landscape is insufficient and advocates for a proactive, interdisciplinary approach, including the integration of "Privacy by Design" principles, to ensure technological advancement is balanced with the unwavering protection of fundamental human privacy.

1. Introduction

Artificial Intelligence in recent times has become a duel-edged sword, as it has brought to the table unprecedented development, as well as threats to privacy and individual security. AI systems, driven by massive datasets, are reshaping industries and social interactions, but they also enable non-consensual data collection, sophisticated synthetic media like deepfakes, and the appropriation of human creations for model training [1, 2]. This review paper synthesizes existing research to analyze the social, legal, and ethical implications of these developments. It explores the mechanisms of AI-driven privacy violations, evaluates the adequacy of current legal frameworks, and discusses emerging technological and policy solutions designed to protect personal data in the digital age.

2. Research Methodology

This review paper is based on a **systematic analysis of secondary data**. The methodology involves:

- **Source Selection**: Prioritizing recent (last 5 years) peer-reviewed journal articles, policy white papers from institutions like Stanford HAI, and government reports. Key sources were identified using the **PRISMA framework** for systematic reviews [1].
- **Comparative Legal Analysis**: Examining and contrasting legal frameworks across different jurisdictions, including the EU AI Act, the U.S. Algorithmic Accountability Act, and India's IT Act, to identify best practices and legislative gaps [2, 6, 8].

Thematic Synthesis: Data from selected sources was coded and analyzed to identify recurring themes and patterns related to AI privacy risks, such as non-consensual data collection, deepfake harms, and intellectual property challenges.

3. AI and Non-Consensual Data Collection

AI systems have an insatiable appetite for data, often collected without meaningful user consent or knowledge. This practice exacerbates existing privacy risks due to the sheer scale and intransparency involved [3].

- **Mechanisms and Risks**: Data is frequently procured through web scraping, interactions with AI applications, and purchases from data brokers [2]. A significant risk is the **repurposing of data**: information shared for one specific purpose, such as a resume or a social media photo, is often used to train AI systems without the user's knowledge or consent [3]. This leads to collection of sensitive personal information, including health and biometric data, increasing the risk of exposure and misuse [2, 4].
- **The Inadequacy of "Opt-Out" Models**: The current default of "opt-out" data collection has been widely criticized. Privacy experts like those at Stanford HAI argue for a fundamental shift to **"opt-in" models**, where user data is not collected without an affirmative choice. The success of Apple's App Tracking Transparency feature, where 80-90% of users choose not to be tracked, demonstrates public preference for greater control [3].
- **Regulatory Responses**: Landmark regulations like the EU's General Data Protection Regulation (GDPR) enforce principles of **data minimization** and **purpose limitation**, requiring companies to collect only necessary data for a specific, lawful purpose [2]. The EU AI Act further prohibits certain practices, such as the untargeted scraping of facial images from the internet to create recognition databases [2].

Risk Category	Description	Real-World Example
Data Collection Without Consent	Scraping or collecting user data without explicit knowledge or permission.	LinkedIn faced backlash after users were auto-opted into AI data training [2].
Repurposing of Data	Using data for a different purpose than what was originally disclosed.	A patient's medical photos, taken for treatment, were used in an AI training dataset without consent [2].
Data Breaches & Leaks	Accidental or malicious exposure of sensitive data used in AI systems.	ChatGPT accidentally revealed users' conversation histories to other users [2].

Table 1: Key AI Privacy Risks and Examples

4. Deepfakes, Misinformation, and Societal Harm

Deepfake technology, which uses AI to create highly realistic synthetic media, represents a profound threat to personal dignity, truth, and social stability [1].

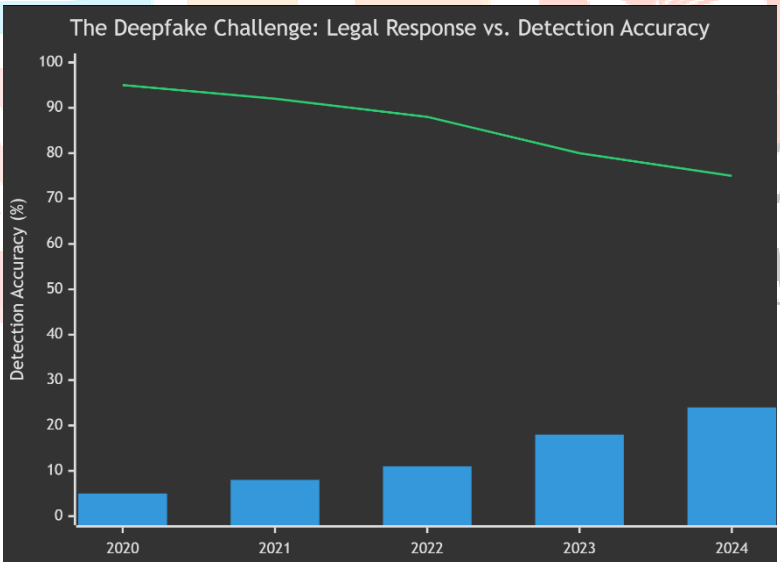

Figure 1: This dual-axis chart shows the simultaneous growth in legal responses (number of U.S. states with laws) and the concerning performance trend of

- **Creation and Misuse**: Deepfakes are primarily created using **Generative Adversarial Networks (GANs)**, where two neural networks work against each other to produce increasingly realistic forgeries [5]. This technology is weaponized for a range of harmful activities, with a disturbing majority—**98% of deepfakes**—being pornographic in nature, overwhelmingly targeting women [1, 6]. Beyond individual harm, deepfakes are used for financial fraud, political misinformation, and identity theft [7, 8].
- **Psychological and Social Impact**: Victims of deepfake abuse experience severe **psychological, social, and professional harm** [1]. The proliferation of synthetic media also erodes the foundation

of trust, leading to a **"decline in trust of visual evidence"** that undermines journalism, legal systems, and public discourse [5].

- **Legal and Detection Countermeasures**: The legal landscape is struggling to keep pace. While over 24 U.S. states have enacted laws against synthetic media, gaps remain globally [1]. Technical solutions are being developed, including:
    - **AI-powered detection tools** to identify synthetic media.
    - **Provenance standards** like the Coalition for Content Provenance and Authenticity (C2PA) that use metadata to track a media item's origin.
    - **Watermarking** (both visible and invisible) to label AI-generated content [1, 7].

5. AI Training and Intellectual Property

The training of AI models on publicly available data, including copyrighted artwork and personal writings, has sparked intense legal and ethical debates.

- **The "Fair Use" Debate**: AI companies often argue that using copyrighted content for training qualifies as transformative **"fair use"** because it involves analysing patterns rather than directly reproducing works. Copyright holders counter that AI systems **compete with original works** and threaten creators' livelihoods [8]. This has led to a surge in litigation, with over 39 copyright-related AI lawsuits currently in U.S. courts [8].
- **Legal Precedents and Gaps**: A pivotal case, **Thomson Reuters v. Ross Intelligence**, found that using copyrighted content to train an AI legal platform constituted infringement, not fair use, signaling how courts might approach these disputes [8]. Existing copyright laws, such as India's Copyright Act of 1957, are often deemed inadequate because they do not explicitly regulate AI-generated content [8].
- **The Human Labor Behind AI**: The development of AI models relies heavily on thousands of **contracted "AI raters"** who perform the often-gruelling work of labelling and correcting data. This invisible human labour is a crucial yet overlooked dimension of AI ethics [8].

6. Privacy Policies and the Accountability of AI Companies

An analysis of AI companies' privacy policies reveals significant disparities in transparency, user control, and data handling practices [2].

- **Loopholes and Opaque Language**: Many privacy policies, particularly from large tech companies, use **vague and overly broad language**, making it difficult for users to understand specific data practices. Critical information is often buried in lengthy documents, and mechanisms to opt out of data collection or model training are either inadequate or non-existent [2].
- **Comparative Privacy Rankings**: A 2025 evaluation of leading AI platforms ranked them based on model training, transparency, and data collection. It found that **Le Chat (Mistral AI)** and **ChatGPT (OpenAI)** demonstrated stronger privacy protections, while **Meta AI** ranked lowest due to vague policies and extensive data sharing [2].
- **Towards Collective Solutions**: Given the scale of data collection, experts argue that an individual rights-based approach to privacy is insufficient. There is a growing push for **collective solutions**, such as **data intermediaries**, which would negotiate data rights on behalf of the public, giving consumers more leverage against large corporations [3].

7. AI Privacy Breaches and Their Impact on Product Design

The principles of data privacy are not merely abstract concerns; they have become foundational to the integrity of modern product design, especially for public-facing platforms. The integration of AI into the design process creates a dual dependency: AI systems enhance design capabilities but also introduce new vulnerabilities where data breaches can corrupt the design process itself, leading to products that are biased, insecure, or fundamentally misaligned with user needs.

7.1. The Role of AI in Modern Product Design

AI is revolutionizing product design by enabling data-driven creativity and efficiency. AI-powered tools can analyze vast datasets, including market trends and user feedback, to generate innovative design concepts and automate the creation of multiple prototypes [9]. This approach allows designers to optimize products for performance, aesthetics, and manufacturing feasibility in a fraction of the traditional time. Furthermore, AI enables "smart design," where user interfaces and experiences (UI/UX) can adapt in real-time to individual user behavior, creating highly personalized and intuitive products [9].

7.2. How Privacy Breaches Corrupt the Design Process

The data-driven nature of AI-powered design makes the process vulnerable to several critical failures if the underlying data is compromised:

Bias Amplification through Tainted Data: If the data used to train design algorithms is collected without consent or is unrepresentative (a common privacy concern), the AI will perpetuate and amplify these biases [10]. This can lead to product designs that systematically disadvantage certain user groups. For instance, a facial recognition feature in a social media app might fail to accurately identify non-consensually collected facial data from underrepresented demographics.

Erosion of User Trust in "Smart" Products: Products that leverage user data for personalization must be built on a foundation of trust. Privacy breaches, such as the repurposing of user data for undisclosed design research, shatter this trust. When users discover their interactions are being used without explicit consent to refine products, their willingness to engage with the platform diminishes, undermining the product's core value proposition [11].

Security-First Design Compromised by Data Theft: The product design of secure platforms, like digital identity wallets, relies on principles like data minimization and encryption to protect users from identity theft [12]. A breach in the AI models used to design these systems—for example, the theft of a dataset used to train authentication algorithms—could expose fundamental security flaws, making the entire product ecosystem vulnerable.

Design Stage	Traditional AI-Driven Approach	Impact of Data Privacy Breaches
Ideation & Research	Analyzes user behavior and feedback to identify needs.	Relies on non-consensually scraped or unrepresentative data, leading to biased product concepts.
Prototyping & Testing	Uses algorithms to generate and simulate countless design variations.	Produces prototypes based on corrupted or incomplete data, resulting in flawed and insecure products.
User Personalization	Tailors the user experience (UX) to individual patterns.	Uses intimate data without clear consent, eroding user trust and leading to reputational damage.

Table 2: How AI Privacy Breaches Impact Different Stages of Product Design

7.3. Integrating Privacy by Design as a Solution

To mitigate these risks, the framework of "Privacy by Design" (PbD) must be integrated into the AI-driven product development lifecycle. PbD is a proactive approach that embeds privacy into the architecture of systems and processes, from the initial design phase through to the final product release [11]. Key practices include:

Conducting Privacy Impact Assessments (PIAs): Before starting a new project, designers and developers should perform a PIA to identify how the AI will process personal data and what privacy risks exist [10, 11].

Adhering to Data Minimization: Product design should collect and use only the data strictly necessary for the specified purpose, avoiding the "over-collection" that AI systems often incentivize [10, 13].

Employing Privacy-Enhancing Technologies (PETs): Techniques like differential privacy (adding statistical noise to data) and federated learning (training algorithms across user devices without centralizing data) can help build products that learn and adapt without directly accessing or storing raw, sensitive user information [11].

8. Conclusion and Future Directions

The intersection of AI and privacy is one of the most critical challenges of the digital era. This review has demonstrated that privacy violations through non-consensual data collection, deepfakes, and unauthorized use of creative works are not mere side effects but inherent risks in the current development paradigm. While regulatory initiatives like the EU AI Act and technical solutions like watermarking and C2PA standards are promising steps, they remain fragmented.

A proactive, **interdisciplinary approach** that integrates technology, law, and ethics is essential [1]. Future efforts must focus on:

- **Comprehensive legal reforms** that specifically criminalize the creation and distribution of non-consensual deepfake content [1].
- **Strengthening global regulatory cooperation** to create harmonized, international standards for AI development and data privacy [7].
- **Investing in public education** to raise awareness about the dangers of deepfakes and the legal recourse available to victims [1].
- **Shifting from opt-out to opt-in data collection models** to return control to users [3].

Furthermore, this analysis has extended the privacy debate to the realm of **product design**, demonstrating that data breaches and unethical data collection do not only harm individuals post-release but can also poison the wellspring of innovation itself. **AI-driven design processes** reliant on biased or non-consensually acquired data risk creating products that are inherently flawed, insecure, and untrustworthy. Therefore, future efforts must focus on:

- **Mandating "Privacy by Design" in AI Development:** Regulators and industry bodies should encourage or require the adoption of PbD frameworks and Privacy Impact Assessments as a standard part of the product development lifecycle for AI systems [11].
- **Building Trust through Transparent Design:** Product designers must prioritize transparency and user control, ensuring that personalization does not come at the cost of privacy, thereby restoring user trust in smart products and platforms.

Only through such coordinated and multifaceted efforts can we hope to build a digital future that is both innovative and respectful of fundamental human privacy.

References:

1. Furizal, N., Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, N., Lonang, S., & Sharkawy, A. (2025). Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review. Social Sciences & Humanities Open, 12, 101882. https://doi.org/10.1016/j.ssaho.2025.101882
2. Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. Frontiers in Digital Health, 7. https://doi.org/10.3389/fdgth.2025.1431246
3. Privacy in an AI era: How do we protect our personal information? | Stanford HAI. (n.d.). https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information
4. Tom, E., Keane, P. A., Blazes, M., Pasquale, L. R., Chiang, M. F., Lee, A. Y., & Lee, C. S. (2020). Protecting data privacy in the age of AI-Enabled ophthalmology. Translational Vision Science & Technology, 9(2), 36. https://doi.org/10.1167/tvst.9.2.36
5. SentinelOne. (2025, October 2). DeepFakes: Definition, Types & Key Examples. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/deepfakes/
6. AI and Data Protection In Pakistan; Outdated State Laws and Vulnerability of Personal Data. (n.d.). https://tils.edu.pk/wp-content/uploads/2025/05/AI-and-Data-Protection-In-Pakistan-Outdated-State-Laws-and-Vulnerability-of-Personal-Data.htm
7. Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. Computer Law & Security Review, 58, 106162. https://doi.org/10.1016/j.clsr.2025.106162

8. Singh, A. (2025, June 10). Deepfake fraud and digital identity theft: A legal analysis under the IT Act, Copyright, and Privacy Laws - the Amikus Qriae. The Amikus Qriae. https://theamikusqriae.com/deepfake-fraud-and-digital-identity-theft-a-legal-analysis-under-the-it-act-copyright-and-privacy-laws/
9. Sreenivasan, A., & Suresh, M. (2024). Design thinking and artificial intelligence: A systematic literature review exploring synergies. International Journal of Innovation Studies, 8(3), 297–312. https://doi.org/10.1016/j.ijis.2024.05.001
10. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems, 34(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885
11. Richter, A. (2025, June 25). How to build trustworthy AI from the ground up with Privacy by Design? TechGDPR. https://techgdpr.com/blog/how-to-build-trustworthy-ai-from-the-ground-up-with-privacy-by-design/
12. Martin, K. D., & Zimmermann, J. (2024). Artificial intelligence and its implications for data privacy. Current Opinion in Psychology, 58, 101829. https://doi.org/10.1016/j.copsyc.2024.101829
13. Pazhohan, H. (2023, July 1). Global Data Protection Standards: A Comparative analysis of GDPR and other international privacy laws. https://jlsda.com/index.php/lsda/article/view/17