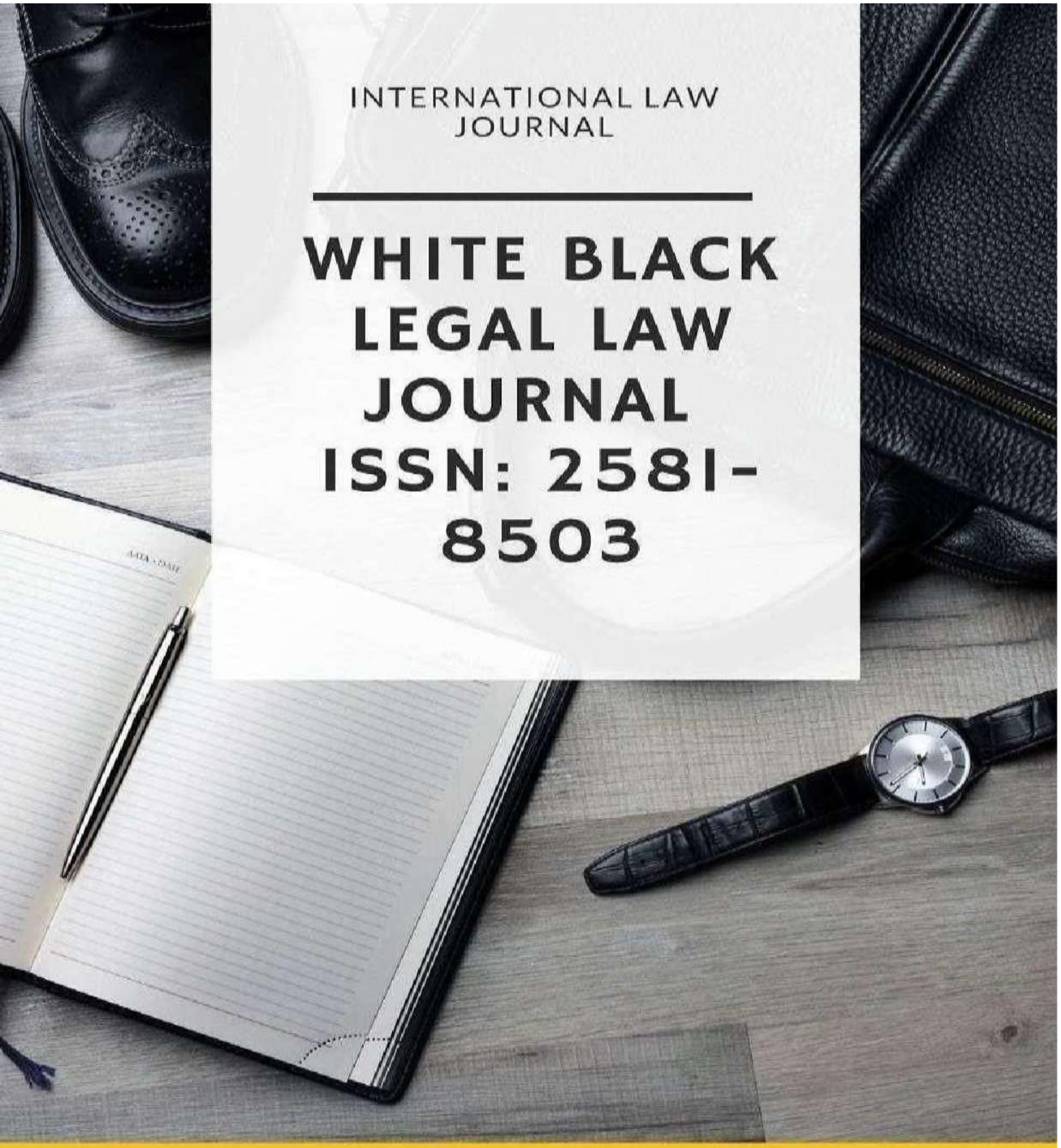

INTERNATIONAL LAW JOURNAL

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.

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.

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

HOW ARTIFICIAL INTELLIGENCE AFFECTS OUR RIGHT TO PRIVACY

AUTHORED BY – RAKESH

Abstract

This paper explores the complex and evolving relationship between artificial intelligence (AI) and the fundamental right to privacy. With AI technologies becoming deeply embedded in everyday life—from digital assistants and targeted advertising to predictive policing and automated hiring decisions—they pose profound challenges to traditional understandings of privacy. These challenges are not merely technological but deeply legal, ethical, and societal. As AI systems demand increasingly vast and varied personal data to function, they simultaneously erode the boundary between public and private spheres, often without explicit user consent or awareness.

The research draws upon a wide array of literature to analyze the multifaceted impacts of AI on privacy. Topics include algorithmic profiling, biometric surveillance, behavioral prediction, and the risks of opaque decision-making processes. The methodology is primarily doctrinal, analyzing statutes such as the GDPR, CCPA, and proposed AI Acts, as well as landmark court decisions and reports from global institutions. This paper argues that existing legal frameworks are inadequate to protect privacy in an AI-driven world and calls for a rights-based, human-centered approach to AI governance. By identifying key risks and proposing actionable solutions, it contributes to the broader discourse on how societies can uphold privacy while embracing the benefits of AI.

Furthermore, the paper identifies gaps in current research, particularly around consent mechanisms, the ethical treatment of inferred data, and the accountability of developers and deployers of AI. With the rise of generative models and synthetic media, privacy challenges are no longer limited to data collected but also include data fabricated using existing personal information. Thus, privacy must be reconceptualized in a world where information can be inferred, recombined, or generated, making legal boundaries difficult to define. The paper concludes with a call for multilateral action, urging regulators, developers, and civil society *to collaborate on creating enforceable, future-proof privacy protections.*

Keywords

Artificial Intelligence, Privacy Rights, Surveillance, Data Protection, Profiling, Legal Frameworks, Ethical AI, GDPR, Facial Recognition, Automated Decision-Making, Data Governance, Predictive Analytics, Synthetic Data, Inference Privacy

Literature Review

The intersection of AI and privacy has been the focus of a growing body of scholarship over the past two decades. Scholars such as Sandra Wachter and Brent Mittelstadt have highlighted the opacity and unpredictability of AI systems, particularly with regard to automated decision-making. Their work stresses the importance of the "right to explanation"—the notion that individuals should be able to understand how algorithmic decisions affecting them are made. Zuboff's theory of "surveillance capitalism" also provides a powerful framework for understanding how data has become the most valuable commodity in the digital economy, often extracted through methods that exploit user ignorance or helplessness.[1]

Daniel Solove offers another critical lens, suggesting that privacy should be understood not merely as the right to secrecy but as the right to control information flows. This shift is crucial in the AI context, where even anonymized data can be re-identified through machine learning techniques. Recent studies by Privacy International and the Electronic Frontier Foundation argue that current data protection regimes fail to anticipate the risks posed by predictive analytics and data inference. Moreover, the World Economic Forum and OECD[2] have issued guidelines urging governments and corporations to adopt AI policies grounded in human rights principles.

The literature also emphasizes the inadequacy of existing legal definitions of harm and consent in the AI era. Scholars such as Lilian Edwards and Woodrow Hartzog have proposed revising legal doctrines to reflect AI's capacity to cause systemic, not just individual, harms. Furthermore, comparative legal analysis reveals a fragmented regulatory landscape: the GDPR provides strong protections but is limited in global reach, while the U.S. approach remains

[1] *Zuboff's theory of "surveillance capitalism"*

[2] *World Economic Forum and OECD*

sector-specific and reactive. This disjointed legal framework hampers international coordination and opens loopholes for exploitation.

In sum, the literature underscores the need for new legal, ethical, and institutional tools to safeguard privacy in the age of AI. These tools must be capable of addressing both immediate and long-term harms, and they must be adaptable to future technological developments. Scholars warn that without urgent reforms; privacy could become a relic of the pre-AI world.

Hypothesis

Artificial Intelligence, by its very design, necessitates the collection and processing of personal data, which makes it inherently invasive to individual privacy rights. The lack of transparency and accountability mechanisms in AI systems exacerbates the risk of privacy violations, leading to potential misuse or abuse of personal data by corporations and governments alike. Therefore, existing privacy laws and frameworks must be updated and expanded to address AI-specific threats to personal privacy.

The hypothesis further posits that without such reforms; AI systems will continue to erode public trust and infringe upon the autonomy of individuals. As algorithmic decision-making becomes more prevalent, the capacity of individuals to understand, challenge, or correct decisions made about them diminishes. This dynamic creates a power imbalance that fundamentally undermines democratic values and human rights.

Introduction

Artificial Intelligence (AI) is reshaping nearly every aspect of our lives—from how we work and shop to how we are governed and even how we communicate. This powerful technology processes massive volumes of personal data to function effectively. While AI offers tremendous benefits in sectors such as healthcare, education, transportation, and finance, it also raises critical concerns about individual privacy. From facial recognition systems and smart assistants to predictive algorithms used in policing, social credit scoring, and automated decision-making in public administration, AI tools frequently operate in opaque ways that users do not fully understand or consent to.[3]

[3] Eubanks, Virginia.*Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, 2018.

The fusion of AI and big data has created new power dynamics where entities that control data hold significant influence, often at the expense of user autonomy and privacy. These entities can include private tech giants, data brokers, governments, and law enforcement agencies. AI enables organizations to monitor behaviors, predict future actions, and even manipulate decisions—transforming data from a passive asset into an active instrument of control. This level of surveillance, often conducted without informed consent, challenges the core principles of privacy and data sovereignty. Moreover, the rapid pace of AI advancement has outstripped the development of legal and ethical frameworks, leaving significant gaps in protection.[4]

As AI becomes embedded in infrastructures such as smart cities, border control, banking, and insurance, its surveillance potential expands. The integration of biometric systems, geolocation tracking, and emotional recognition software is turning AI into a mechanism of continuous data extraction. Many of these technologies are introduced under the pretense of safety, efficiency, or personalization, thereby masking the privacy risks they impose. Importantly, individuals often cannot opt out of these systems, especially when AI is used by public authorities. This involuntary participation underscores the asymmetry of power and the inadequacy of traditional consent models.[5]

These factors necessitate a comprehensive exploration of how AI impacts privacy, the ethical implications of its deployment, and the legal mechanisms available to safeguard individual rights in the digital age. The discussion must also consider the international dimension of AI governance, including global disparities in privacy standards and the transboundary nature of data flows. From the EU's stringent privacy laws to the surveillance-oriented approaches of some authoritarian regimes, there is a wide spectrum of regulatory philosophies. Only by critically examining these intersections can societies hope to build AI systems that respect, rather than undermine, the foundational human right to privacy.[6]

What is AI privacy?

AI privacy is the practice of protecting personal or sensitive information collected, used, shared or stored by AI.

[4] Zuboff, Shoshana. *The Age of Surveillance Capitalism.* PublicAffairs, 2019

[5] Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review*, Vol. 126, 2013.

[6] van Dijck, José. *The Culture of Connectivity: A Critical History of Social Media.* Oxford University Press, 2013.

AI privacy is closely linked to data privacy. Data privacy, also known as information privacy, is the principle that a person should have control over their personal data. This control includes the ability to decide how organizations collect, store and use their data. But the concept of data privacy predates AI and how people think of data privacy has evolved with the advent of AI.

“Ten years ago, most people thought about data privacy in terms of online shopping. They thought, ‘I don't know if I care if these companies know what I buy and what I'm looking for, because sometimes it's helpful,’” Jennifer King, a fellow at the Stanford University Institute for Human-Centered Artificial Intelligence, explained in an interview posted to the institute’s website.[7]

“But now we've seen companies shift to this ubiquitous data collection that trains AI systems,” King said, “which can have major impact across society, especially our civil rights.”

Understanding the privacy risks of AI

We can often trace AI privacy concerns to issues regarding data collection, cybersecurity, model design and governance. Such AI privacy risks include:

- Collection of sensitive data
- Collection of data without consent
- Use of data without permission
- Unchecked surveillance and bias
- Data exfiltration
- Data leakage

Collection of sensitive data

One reason AI arguably poses a greater data privacy risk than earlier technological advancements is the sheer volume of information in play. Terabytes or petabytes of text, images or video are routinely included as training data, and inevitably some of that data is sensitive: healthcare information, personal data from social media sites, personal finance data, biometric data used for facial recognition and more. With more sensitive data being collected, stored and transmitted than ever before, the odds are greater that at least some of it will be exposed or

[7] Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of Machine Learning Research.

deployed in ways that infringe on privacy rights.[8]

Collection of data without consent

Controversy may ensue when data is procured for AI development without the express consent or knowledge of the people from whom it's being collected. In the case of websites and platforms, users increasingly expect more autonomy over their own data and more transparency regarding data collection. Such expectations came to the fore recently, as the professional networking site LinkedIn faced backlash after some users noticed they were automatically opted into allowing their data to train generative AI models.[9]

Use of data without permission

Even when data is collected with individuals' consent, privacy risks loom if the data is used for purposes beyond those initially disclosed. "We're seeing data such as a resume or photograph that we've shared or posted for one purpose being repurposed for training AI systems, often without our knowledge or consent," King said. In California, for instance, a former surgical patient reportedly discovered that photos related to her medical treatment had been used in an AI training dataset. The patient claimed that she had signed a consent form for her doctor to take the photos, but not for them to be included in a dataset.[3]

Unchecked surveillance and bias

Privacy concerns related to widespread and unchecked surveillance—whether through security cameras on public streets or tracking cookies on personal computers—surfaced well before the proliferation of AI. But AI can exacerbate these privacy concerns because AI models are used to analyze surveillance data. Sometimes, the outcomes of such analysis can be damaging, especially when they demonstrate bias. In the field of law enforcement, for example, a number of wrongful arrests of people of color have been linked to AI-powered decision-making.[4]

Data exfiltration

AI models contain a trove of sensitive data that can prove irresistible to attackers. "This [data] ends up with a big bullseye that somebody's going to try to hit," Jeff Crume, an IBM Security

[8] Brundage, M., Avin, S., Clark, J., et al. (2020). *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*. arXiv preprint.

[9] Carlini, N., Tramer, F., Wallace, E., et al. (2021). *Extracting Training Data from Large Language Models*. arXiv preprint arXiv:2012.07805.

Distinguish Engineer, explained in a recent IBM Technology video (the link resides outside ibm.com). Bad actors can conduct such data exfiltration (data theft) from AI applications through various strategies. For instance, in prompt injection attacks, hackers disguise malicious inputs as legitimate prompts, manipulating generative AI systems into exposing sensitive data. Such as, a hacker using the right prompt might trick an LLM-powered virtual assistant into forwarding private documents.[10]

Data leakage

Data leakage is the accidental exposure of sensitive data, and some AI models have proven vulnerable to such data breaches. In one headline-making instance, ChatGPT, the large language model (LLM) from OpenAI, showed some users the titles of other users' conversation histories.[5] Risks exist for small, proprietary AI models as well. For example, consider a healthcare company that builds an in-house, AI-powered diagnostic app based on its customers' data. That app might unintentionally leak customers' private information to other customers who happen to use a particular prompt. Even such unintentional data sharing can result in serious privacy breaches.[11]

Importance of Privacy in the Digital Era

In the digital era, personal data has become an incredibly valuable commodity. The vast amounts of data generated and shared online daily have enabled businesses, governments, and organisations to gain new insights and make better decisions. However, this data also contains sensitive information that individuals may not want to share or organisations have used without their consent.[12] That is where privacy comes in.

Privacy is the right to keep personal information confidential and free from unauthorised access. It is an essential human right that ensures individuals have control over their personal data and how it is used. Today, privacy is more important than ever as the amount of personal data collected and analysed continues to grow.[13]

Privacy is crucial for a variety of reasons. For one, it protects individuals from harm, such as

[10] Solove, D. J. (2006). *A Taxonomy of Privacy*. University of Pennsylvania Law Review, 154(3), 477–560.
[11] Wired. (2023). *Patient's Medical Photos Used in AI Dataset Without Permission*.
[12] Daniel J Solove, *Understanding Privacy* (Harvard University Press 2008).
[13] UN General Assembly, *Universal Declaration of Human Rights* (adopted 10 December 1948) 217 A(III), art 12.

identity theft or fraud. It also helps to maintain individual autonomy and control over personal information, which is essential for personal dignity and respect. Furthermore, privacy allows individuals to maintain their personal and professional relationships without fear of surveillance or interference. Last but not least, it protects our free will; if all our data is publicly available, toxic recommendation engines will be able to analyse our data and use it to manipulate individuals into making certain (buying) decisions.

In the context of AI, privacy is essential to ensure that AI systems are not used to manipulate individuals or discriminate against them based on their personal data. AI systems that rely on personal data to make decisions must be transparent and accountable to ensure that they are not making unfair or biased decisions.[14]

The importance of privacy in the digital era cannot be overstated. It is a fundamental human right that is necessary for personal autonomy, protection, and fairness. As AI continues to become more prevalent in our lives, we must remain vigilant in protecting our privacy to ensure that technology is used ethically and responsibly.

How Does AI Collect Your Data? It Listens!

AI systems gather data through various inputs, including voice assistants (like Alexa or Siri), smartphone sensors, GPS, social media, wearable devices, and smart home appliances. These systems "listen" not just in the auditory sense but through constant data collection from interactions and behaviors. AI-enabled applications monitor clicks, keystrokes, app usage patterns, and even biometric data to learn about the user. This massive and passive data acquisition often occurs without explicit consent, raising questions about informed participation and ethical design.[15]

Beyond these inputs, AI also collects metadata and contextual information. For example, facial recognition cameras track movement patterns in public places, while AI in vehicles logs driving behaviour and routes. Algorithms scrape content from social media, emails, and text messages to build detailed user profiles. The vast scale of data collection, often unregulated and unnoticed, allows AI to create an intimate digital portrait of individuals—including their habits,

[14]

[15] Karen Yeung, 'Hypernudge: Big Data as a Mode of Regulation by Design' (2017) 20 *Information, Communication & Society* 118.

preferences, relationships, and even emotions.[16] This level of surveillance, largely invisible to users, significantly erodes the boundary between public and private life.

How AI Uses This Data

Once collected, AI systems process personal data using algorithms designed to recognize patterns, predict behaviors, and automate decisions. In advertising, this data is used to create hyper-targeted campaigns. In healthcare, AI analyzes patient data to assist in diagnosis and treatment. Law enforcement agencies use facial recognition data for tracking suspects.[17] However, this usage raises ethical concerns—especially when individuals are unaware of how their data is being used or when AI decisions affect access to loans, jobs, or even liberty.

Furthermore, AI systems often combine data from multiple sources to infer new information. For instance, combining location data with browsing history can predict political affiliation, sexual orientation, or mental health status. These inferences, though powerful, are rarely subject to user control or verification. This creates a risk of misclassification and discrimination, especially when such data is used in critical areas like hiring, insurance underwriting, or criminal justice.[18] The opaque nature of algorithmic processes further compounds the problem, as affected individuals have limited avenues for redress or appeal.

AI Surveillance and Facial Recognition

Facial recognition technologies powered by AI have introduced new forms of surveillance. These systems can identify individuals in real time, monitor movements, and even analyze emotions. While some applications are beneficial (e.g., identifying missing persons), others infringe on civil liberties. In countries like China, AI is used to assign social scores, while in the U.S. and U.K., police departments have deployed facial recognition in ways that raise concerns about racial bias and wrongful arrests.[19]

Such surveillance technologies are often implemented without public debate or oversight. They disproportionately impact marginalized communities, who are more likely to be misidentified

[16] Brent Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 *Big Data & Society* 1.

[17] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34 *Computer Law & Security Review* 436.

[18] Cathy O’Neil, *Weapons of Math Destruction* (Crown 2016)

[19] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology 2016).

and subjected to surveillance. This trend has led to calls for bans or moratoriums on facial recognition technology, especially in democratic societies. The chilling effect on free speech, assembly, and association is another serious concern. As AI-powered surveillance becomes ubiquitous, it risks normalizing a culture of constant observation, undermining the foundational principles of privacy and freedom.[20]

Legal and Ethical Implications

Many jurisdictions lack robust legal frameworks specifically governing AI. The EU's GDPR and the upcoming AI Act attempt to regulate AI by introducing transparency, accountability, and risk classification. In contrast, other regions operate in legal vacuums. Ethical concerns include the need for informed consent, user autonomy, algorithmic bias, and the opaque nature of decision-making. These issues call for the development of ethical standards and regulatory oversight to ensure that AI respects fundamental human rights.

There is also an urgent need to clarify the legal status of algorithmic decisions. Current laws often treat AI as a tool rather than an agent, which complicates liability and accountability. Should a facial recognition error lead to wrongful arrest, it is unclear whether the fault lies with the software provider, the law enforcement agency, or the developer. Moreover, the cross-border nature of AI complicates enforcement, as data often flows across jurisdictions with varying privacy protections. Ethical frameworks must also grapple with issues like data ownership, the right to explanation, and digital consent.[21]

Potential Solutions to AI and Data Privacy

Several solutions can address AI’s privacy risks. One approach is incorporating privacy-by-design and privacy-by-default principles into AI systems. Technologies such as federated learning and differential privacy allow data analysis without compromising individual identities.[22] Laws must be updated to require meaningful consent and algorithmic transparency. Public awareness campaigns and digital literacy programs are also essential to empower individuals to control their data. Finally, international cooperation is needed to create harmonized AI governance.

[20] Amnesty International, 'Ban the Scan: Facial Recognition Technology Fuels Racist Policing' (2021).

[21] AI Now Institute, *AI Now 2018 Report* (New York University 2018).

[22] Cynthia Dwork and Aaron Roth, ‘The Algorithmic Foundations of Differential Privacy’ (2014) *Foundations and Trends in Theoretical Computer Science* 1.

Another potential solution lies in promoting open-source and auditable AI systems. Transparency can be achieved by enabling independent experts to review algorithmic models and datasets. Data trusts and cooperative models can give users greater control over how their data is used. Regulatory sandboxes may also help governments experiment with new legal tools for AI oversight. Additionally, AI ethics boards and citizen panels can ensure that diverse perspectives inform the development and deployment of AI systems. These strategies, taken together, can foster a privacy-respecting AI ecosystem.

Comparative International Approaches

The European Union stands out with the General Data Protection Regulation (GDPR), offering the most comprehensive privacy rights to individuals, including the right to access, correct, delete, and port data. The proposed AI Act adds another layer of control by regulating high-risk AI applications. The U.S., in contrast, lacks a federal law, relying on sectoral rules. China emphasizes surveillance and state control over privacy. This global disparity highlights the urgent need for harmonized regulations that prioritize human dignity.[23]

Other countries are also experimenting with unique frameworks. Canada has proposed a Digital Charter Implementation Act that seeks to modernize privacy laws in the digital age. Brazil’s General Data Protection Law (LGPD) is modeled after the GDPR but tailored to local realities. India has introduced a Personal Data Protection Bill, which, if enacted, will create a dedicated authority to oversee data governance.[24] These efforts reflect a growing international consensus on the need for AI regulation but also reveal differences in priorities and approaches. Cross-border collaboration and treaty-based frameworks may offer a path forward.[25]

Conclusion

Artificial Intelligence has brought transformative capabilities but also unprecedented challenges to privacy. AI systems thrive on personal data, making it both a tool for innovation and a potential weapon for intrusion. As the technology evolves, so too must our legal, ethical, and technological safeguards. Comprehensive regulations, ethical design principles, and public empowerment are essential to strike a balance between innovation and individual rights. If

[23] Samm Sacks, ‘Data Control and Cybersecurity in the Chinese State’ (2019)
[24] Government of Canada, 'Digital Charter Implementation Act, 2020
[25] OECD, 'Recommendation on Artificial Intelligence' (2019).

privacy is to be preserved in the digital age, AI must be guided by transparency, accountability, and respect for human dignity.

The stakes are high: failure to address AI's privacy risks could lead to a future of mass surveillance, algorithmic discrimination, and loss of autonomy. Conversely, thoughtful governance can enable the responsible use of AI that enhances, rather than threatens, our fundamental rights. As we move forward, a multi-stakeholder approach—involving governments, industry, civil society, and the public—will be critical to shaping an AI future that respects privacy and fosters trust.

Bibliography

1. *Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) 376 Philosophical Transactions of the Royal Society A 20180089.*
2. *Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019(2) Columbia Business Law Review 494.*
3. *European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)' [2016] OJ L119/1.*
4. *European Commission, 'Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' COM (2021) 206 final.*
5. *Jennifer King, 'AI and Privacy: What Do We Really Know?' (Stanford HAI, 2023)*
6. *Daniel J Solove, Understanding Privacy (Harvard University Press 2008).*
7. *Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (Harvard University Press 2018).*
8. *IBM, 'How AI Poses New Risks to Data Privacy' (IBM Technology, 2023)*
9. *Kashmir Hill, 'Wrongfully Accused by an Algorithm' The New York Times (24 June 2020*
10. *Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs 2019).*