ABUAD Law Journal (ALJ)
Vol. 12, ISSUE 1, 2024, Pages 41-64 https://doi.org/10.53982/alj.2024.1201.03-j
Published by College of Law, Afe Babalola University Law Journal,
College of Law, Afe Babalola University, Km 8.5, Afe Babalola Way,
P.M.B. 5454, Ado Ekiti, Ekiti State, Nigeria ISSN: *2971-7027*
www.abuad.edu.ng, abuadlawjournal@abuad.edu.ng

AI AND PERSONAL DATA PRIVACY IN THE U.S: BALANCING CUSTOMER CONVENIENCE WITH PRIVACY COMPLIANCE.

Hakeemat Ijaiya* and Israel Adekunle Adeniyi**

Abstract

The proliferation of Artificial Intelligence (AI) across various industries in the United States has ushered in an era of transformative technological advancements, which has provided businesses with the ability to enhance customer experiences and drive operational efficiencies. However, this development has brought about increased challenges in preserving the privacy and security of personal data in the US. The paper examines the need to balance customer convenience with privacy compliance within the context of AI and personal data privacy in the U.S. The paper also examines the state of data privacy and concerns arising from the use of AI. It assesses the key legal frameworks in the U.S. and their adequacy to regulate AI in light of data privacy. The paper employs a doctrinal research methodology to examine the laws and identify the challenges arising from the regulatory gaps in AI and personal data privacy. The paper finds that there are challenges stemming from the lack of alignment between existing legal frameworks and the evolving AI technologies, especially in relation to data collection, data anonymization, and consent management. The paper recommends the need to reform existing laws to be up to date with the evolving capabilities of AI. The paper concludes that the growth of AI in relation to personal data privacy presents both opportunities and challenges.

Introduction

In recent years, the widespread adoption of AI has rapidly transformed industries, from healthcare and finance to e-commerce and entertainment.[1] Not only has the advent of AI led to efficiency in operations but also altered the way businesses interact with their customers.[2] With AI, businesses can now, at the speed of light, analyse vast amounts of data, predict consumer behaviour, personalize user experiences, and automate various tasks.[3] For instance, Amazon uses AI to personalise its product recommendations and cashier-less Amazon Go stores.[4] Alibaba utilises AI-powered chatbots to assist consumers and optimise search results on its platform.[5] Also, eBay employs AI for cataloguing and sorting millions of products listed on their platform.[6] Essentially, for these platforms, AI powers a multitude of applications and drives technological innovations which have undeniably improved the online shopping experience of their users. AI has brought convenience, personalisation, and efficiency to ecommerce like never before.[7] AI

*LLM Indiana University, Indianapolis, USA; hakeematijaiya@gmail.com
*Faculty of Law, University of Ilorin, Nigeria; israeladeniyi178@gmail.com

[1] Ali Y., and others, 'A systematic literature review of artificial intelligence in the healthcare sector: Benefits, challenges, methodologies, and functionalities' *Journal of Innovation & Knowledge* (2023) 8(1) 100333; Dwivedi Y., and others., 'Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions' *Technological Forecasting and Social Change* (2023) 192, 122579; Hasan A., 'Artificial Intelligence (AI) in Accounting & Auditing: A Literature Review', *Open Journal of Business and Management* (2022) 10(1) 441.

[2] Enholm I., and others,., 'Artificial Intelligence and Business Value: A Literature Review', *Information Systems Frontiers* (2022) 24 1709.

[3] Kietzmann, J., Paschen, J., and Treen, E., 'Artificial intelligence in advertising: how marketers can leverage artificial intelligence along the consumer journey,' *J. Advert. Res*., (2018) 58(3) 263; Haddon H. and Stevens L., 'Amazon Test Its Cashierless Technology for Bigger Stores'*The Wall Street Journal* (New York, 2 December, 2018) <https://www.wsj.com/articles/amazon-tests-its-cashierless-technology-for-bigger-stores-1543776320> accessed 04 November, 2023;

[4] Estiak Monjur, and others, 'The Impact of Artificial Intelligence on International Trade: Evidence from B2C Giant E-Commerce (Amazon, Alibaba, Shopify, eBay).' *Open Journal of Business and Management* (2023) 11(5) 10.4236/ojbm.2023.115132.

[5] Ibid.

[6] Bernard Marr, 'The Amazing Ways eBay Is Using Artificial Intelligence to Boost Business Success' Forbes (New Jersey, 26 April 2019) <https://www.forbes.com/sites/bernardmarr/2019/04/26/the-amazing-ways-ebay-is-using-artificial-intelligence-to-boost-business-success/?sh=48a5c88e2c2e> accessed 04 November, 2023.

[7] See Harrigan P., 'How Amazon Uses AI to Dominate Ecommerce: Top 5 Use Cases' *GoDataFeed* (USA, 17 November, 202) <https://www.godatafeed.com/blog/how-amazon-uses-ai-to-dominate-ecommerce> accessed 04 November, 2023;; Qin Y., and others, 'Artificial Intelligence and Economic Development: An Evolutionary Investigation and Systematic Review' *Journal of Knowledge Economics* (2023) 14(2) 3; Kolodin, D. and others,

has therefore become an engine of innovation and competitiveness in the global marketplace. Allioui and Mourdi stated that the growing influence of AI cannot be overstated, and its applications continue to expand rapidly.[8] For instance, in the retail sector, AI-powered recommendation engines analyse customer browsing and purchase history to suggest products tailored to individual preferences.[9] In the finance, AI algorithms are utilized for fraud detection, risk assessment, and algorithmic trading.[10] In healthcare, AI is transforming patient care with predictive analytics, image recognition, and diagnostic support.[11] AI's impact is not limited to the private sector. Government agencies employ AI for enhancing public services, such as optimizing traffic flow and predicting disease outbreaks.[12] In law, AI aids in contract analysis, legal research, and document automation. The breadth of AI applications is an indication of its role in the present and future of various facets of life.[13]

As AI advances, the need to safeguard personal data from unauthorized access, breaches, and misuse has never been more critical. Most especially, in the US, the significance of personal data privacy has grown exponentially. The U.S. is home to numerous tech giants and start-ups, making it a hub of personal information of millions of individuals. Personal information in this context includes not only names and addresses but also sensitive medical records, financial transactions, and behavioural patterns. Laws such as the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA) lay the foundation for safeguarding personal information. Additionally, international standards like the

---

'Artificial Intelligence in E-Commerce: Legal Aspects' *Advances in Economics, Business and Management Research* (2020) 129(3) 96.

[8] Allioui, H. and Mourdi. Y., 'Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey,' *Sensor*s, (2023) 23(19) 8015 https://doi.org/10.3390/s23198015

[9] Necula, S. and Păvăloaia, V., 'AI-Driven Recommendations: A Systematic Review of the State of the Art in E-Commerce,' *Appl. Sci.,* (2023) 13(9) 5531, https://doi.org/10.3390/app13095531

[10] Kaur, K., Kumar, Y., and Kaur, S., 'Artificial Intelligence and Machine Learning in Financial Services to Improve the Business System,' in Kautish, P., and others., *Computational Intelligence for Modern Business Systems: Disruptive Technologies and Digital Transformations for Society 5.0* (Springer, Singapore, 2024) 3-30.

[11] Davenport T. and Kalakota R., 'The potential for artificial intelligence in healthcare,' *Future Healthcare Journal*, (2019) 6(2) 94–98; Herath, H.M. and Mittal, M., 'Adoption of artificial intelligence in smart cities: A comprehensive review' *International Journal of Information Management Data Insights* (2022) 2(1) 100076. <https://doi.org/10.1016/j.jjimei.2022.100076> accessed 4th November, 2023

[12] Chakrabarti, S.and Ray R., 'Artificial Intelligence And The Law' *Journal of Pharmaceutical Negative Results*, (2023) 14 (2) 87-96.

[13] Ibid.

European Union's General Data Protection Regulation (GDPR) influence U.S. businesses operating globally. While the US legal framework features a patchwork of federal and state-level regulations addressing data privacy, the importance of data privacy extends beyond mere compliance. It is rather tied to the trust that individuals place in organizations that collect and process their information. In an era where data breaches and privacy scandals are front-page news, consumers are increasingly concerned about the security and privacy of their personal data.

In this era of AI, businesses face a challenging dichotomy: how to increase customer convenience through AI-driven services while ensuring the privacy and security of customer data.[14] The convenience of personalized recommendations, voice-activated assistants, and frictionless transactions is highly appealing to consumers. However, delivering these conveniences often entails the collection, storage, and analysis of vast amounts of personal data This balance is not only a legal and ethical matter but also a competitive one.[15] Companies that can handle the complexities of data privacy effectively stand to gain a competitive edge by increasing consumer trust and loyalty. Conversely, those that neglect data privacy can incur substantial fines, legal liabilities, and reputational damage.

The globalized nature of data flow, especially in multinational business operations, presents intricate challenges regarding data privacy. The US legal framework faces difficulties aligning with international standards, such as the GDPR, due to differing approaches to data privacy. This lack of alignment has often times resulted in complexities and inconsistencies in data transfer mechanisms across borders. Such discrepancies can lead to legal ambiguities and potential vulnerabilities in safeguarding personal data, particularly when it traverses international boundaries, raising concerns about data security and privacy breaches.

Moreover, the increasing autonomy of AI systems in decision-making processes amplifies the complexity of defining liability and accountability. Existing legal frameworks often lack explicit

[14] Deryl, M. D., Verma, S., and Srivastava, V., ‚How does AI drive branding? Towards an integrated theoretical framework for AI-driven branding.’ (2023) 3(2) *International Journal of Information Management Data Insights*, 100205.

[15] Perifanis, N. and Kitsios F., 'Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review,' *Information* (2023) 14(2) 85 https://doi.org/10.3390/info14020085.

guidelines on attributing responsibility when AI-driven decisions impact individuals' rights. Take for instance, the California Consumer Privacy Act is currently the most comprehensive data privacy law in the US.[16] As comprehensive as it currently is, it lacks provisions that guide "automated decision-making" in AI-enabled technologies.[17] This is why the California Privacy Protection Agency has proposed guidelines that will regulate automated decision making and profiling for big companies that process consumer data.[18] Provisions that attribute responsibility when AI-enabled decisions affect individuals' rights are also non-existent in the Act.. . This legal gap raises concerns about legal accountability in scenarios where AI systems make critical decisions that affect individuals, such as in healthcare, finance, or employment. The absence of clear regulatory directives regarding accountability in AI-driven decision-making could lead to legal uncertainties and challenges in determining culpability in case of adverse outcomes. This paper examines the implications of AI on data privacy. It analyses the prominent legal framework on data privacy in the US and its adequacy to regulate AI.

Data Privacy Concerns Arising from AI

Industries that were once reliant on manual processes are now harnessing AI to streamline operations and drive growth.[19] Especially in customer-centric industries, AI has emerged as a game-changer. It has changed the way businesses engage with consumers. AI algorithms are now used to analyse past purchase history, browsing patterns, and even external factors like weather or trends to recommend products based on individual preferences.[20] In e-commerce, chatbots are now used to provide real-time customer support, address inquiries, resolve issues, and even guide

[16] Fath, K.R. and Oberly, D.J., 'California Privacy Protection Agency Continues Rulemaking Focus on Automated Decision-Making and Profiling in Stakeholder Sessions' *National Law Review* (Illinois, 2022) <https://natlawreview.com/article/california-privacy-protection-agency-continues-rulemaking-focus-automated-decision> accessed 20th April, 2024.

[17] See Johnson, K., 'California Privacy Agency Advances AI Rules to Protect Consumer Data' *KQED* (USA, 2023). <https://www.kqed.org/news/11979306/california-takes-steps-to-regulate-ai-use-by-large-companies> accessed 23rd April, 2024.

[18] Ibid.

[19] Mikalef, P. and others., 'Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective' *Journal of Business Research* (2023) 164, 113998.

[20] Soori, M., Arezoo, B. and Dastres, R., 'Artificial intelligence, machine learning and deep learning in advanced robotics, a review' *Cognitive Robotics* (2023) 3, 54-70.

customers through the purchasing process.[21] These chatbots are capable of understanding natural language and can operate around the clock to ensure a seamless and efficient interaction with consumers. This level of personalization enhances customer experience and drives sales and customer loyalty. The benefits of AI-driven consumer convenience are boundless. It increases the likelihood of consumers finding products or services that genuinely interest them, leading to high conversion rates. AI boosts consumer satisfaction and reduces the burden on consumer support teams.

AI is a game-changer in the e-commerce industry.[22] It has fundamentally altered the way consumers interact with online shopping platforms. It has enabled businesses to optimise product recommendations, manage inventory, and enhance overall business efficiency.[23] One of the standout applications of AI in e-commerce is machine learning, which drives the engine behind personalised product recommendations.[24] AI algorithms analyse vast troves of customer data, such as browsing history, past purchases, and demographic information, to provide tailored product suggestions. This not only streamlines the shopping process but also enhances customer satisfaction, as individuals are more likely to discover products aligning with their preferences. For example, a consumer searching for a laptop may receive recommendations for complementary accessories or similar tech gadgets.

Data collected from consumers are typically stored in databases and can be accessed in real-time to deliver AI-driven services.[25] However, the collection and storage of personal data raise critical privacy concerns. The more data that businesses accumulate, the greater the responsibility they have to safeguard it from breaches and misuse. As AI systems continuously learn and adapt, they require access to historical and real-time data. This backdrop necessitates the importance of

[21] See Adam, M., Wessel M., and Benlian A., 'AI-based Chatbots in Customer Service and Their Effects on User Compliance' *Electronic Markets* (2021) 31, 427–445.

[22] Bawack R., and others, 'Artificial intelligence in E-Commerce: a bibliometric study and literature review' *Electron Markets* (2022) 32, 297.

[23] Perifanis, N. and Kitsios, F., 'Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review' *Information* (2023) 14(2), 85.

[24] Bawack R., and others, see note 17 above, p. 300.

[25] Barja-Martinez S., and others, 'Artificial Intelligence techniques for enabling Big Data services in distribution networks: A review' *Renewable and Sustainable Energy Reviews* (2021) 150, 111459. <https://doi.org/10.1016/j.rser.2021.111459> accessed 24th November, 2024.

robust data privacy measures. The concerns, which any data privacy measures will address, are several.

In terms of surveillance, the use of AI often involves systematic digital surveillance across most facets of life.[26] AI has revolutionized surveillance by enabling real-time analysis and processing of every frame from millions of cameras. AI-powered tools are opening new frontiers in state surveillance around the world.[27] These tools can identify faces, track movements, and even analyze public sentiment online. They can also detect irregular behavior and identify dangerous activity that might be ignored by a human.[28] The issue with this is that the vast amounts of data collected by AI surveillance systems can be misused, especially when it falls into the wrong hands.[29] For instance, AI surveillance can be used to map, track, and control people to meet various policy aims, some of which may violate human rights. AI surveillance can also lead to data exploitation. Personal data, including sensitive information, can be exploited by businesses for marketing insights or sold to other companies.[30] AI surveillance technologies, such as facial recognition and vehicle recognition, can swiftly identify potential threats and security breaches, but these technologies also enable tracking of individuals' locations and habits, raising privacy concerns.

Data minimisation is another concern that the use of AI raises. AI systems are often data-hungry, collecting more information than necessary. This practice contradicts the principle of data minimization, which advocates for collecting only data that is adequate, relevant, and necessary.[31] The principle of data minimization is a core part of global data privacy laws like the

[26] Ergashev, A., 'Privacy concerns and data protection in an era of ai surveillance technologies.' *International Journal of Law and Criminology* (2023) 3(8), 71-76.
[27] Karpa, D., Klarl, T., and Rochlitz, M., 'Artificial intelligence, surveillance, and big data.' In Lars Hornuf (ed.) *Diginomics Research Perspectives: The Role of Digitalization in Business and Society* (Cham: Springer International Publishing, 2022) pp. 145-172.
[28] Ibid.
[29] Ergashev, A. (see note 21 above).
[30] Dilmaghani, S., and others, 'Privacy and security of big data in AI systems: A research and standards perspective.' In *2019 IEEE international conference on big data (big data)* (pp. 5737-5743). IEEE.
[31] Biega, A. J., and Finck, M., 'Reviving purpose limitation and data minimisation in data-driven systems.' *arXiv preprint arXiv:2101.06203* (2021) <https://arxiv.org/abs/2101.06203> accessed 24th April, 2024.

GDPR.[32] It aims to limit the incentives for unbridled commercial surveillance practices, including restrictions on what data is collected (collection limitations), the purposes for which it can be used following collection (purpose limitations), and the amount of time firms can retain data (storage limitations).[33] While AI systems require vast amounts of data to learn, make predictions, and improve their performance, the extensive data collection can lead to the accumulation of unnecessary or irrelevant data. AI systems can thus exacerbate known security risks and make them more difficult to manage because compliance with data protection law's security requirements can be more challenging with AI than with other, more established technologies.[34] Notwithstanding this concern, Biega and Finck believe that the next generation of data minimization policies—bright-line rules that prohibit excessive or harmful data collection and use—show greater promise as they could be a powerful lever in restraining some of the most concerning AI systems.[35]

As against the ethical principle of storage limitation, which states that the duration of data storage should be limited, in AI-driven technologies, there is prolonged data storage, which increases the risk of data breaches and unauthorized access. Ethically speaking, once the data is no longer required for that specific purpose, it should be deleted or anonymized.[36] Although AI systems are data-driven, their effectiveness and accuracy largely depend on the availability and evaluation of data.[37] These systems have an enormous 'appetite for data', and the accumulation of relevant (personal or non-personal) data regularly constitutes a key factor for AI-related issues.[38] Moreover, storage limitation poses considerable difficulties in AI constellations, because the deletion or restriction of personal data significantly limits the output of AI-based

[32] Ibid.
[33] Ibid.
[34] Malek, M. A., 'Bigger Is Always Not Better; less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data.' *Eur. J. Privacy L. & Tech.*, (2021) 212.
[35] Biega, A.J. AND Finck, M., (see note 26 above).
[36] Wong, C. H., Samad, M. A., and Taib, N., 'Potential and limitation of AI system in building services and control management system.' In *IOP Conference Series: Earth and Environmental Science* (2021) Vol. 881, No. 1, p. 012044.
[37] Biega, A.J. and Finck,M. (see note 26 above).
[38] Wong, C.H. Samad, M.A. and Taib, N. (see note 30 above).

application.[39] This necessitates the development of robust data governance strategies and the implementation of effective data protection measures.

The issue of purpose limitation is also relative in AI-driven businesses. Purpose limitation is fundamental in data protection and privacy because it mandates that data collected for one purpose should not be used for another unless additional notice is given and consent is obtained.[40] As previously stated, AI systems are inherently data-driven, and their effectiveness largely depends on the availability and evaluation of data. However, these systems often repurpose data without user knowledge or consent, which can lead to what is known as 'function creep', particularly when data is used beyond its originally specified, explicit, and legitimate purposes.[41] For instance, an AI system intended for specific crime prevention goals might gradually be repurposed for unwarranted surveillance activities not originally considered, which violates the principle of purpose limitation and raises significant ethical and privacy concerns. In addressing this concern, To address this issue, scholars like Muhlfhoff and Ruschemeier have proposed a novel approach to AI regulation, introducing what is termed 'purpose limitation for training and reusing AI models' to mandate that those training AI models define the intended purpose (e.g., "medical care") and restrict the use of the model solely to this stated purpose.[42]

AI systems, when not adequately regulated, are indeed susceptible to data misuse and compromise. AI systems often require vast amounts of data for training and operation, but, if this data is not properly managed or protected, it can be exploited for antisocial purpose.[43] For instance, AI tools trained with data scraped from the internet can inadvertently memorize personal information about individuals, which could potentially enable identity theft or fraud. The features that make AI and Machine Learning (ML) systems integral to businesses, such as

[39] Walton, P., 'Artificial intelligence and the limitations of information.' *Information* (2018) 9(12), 332.
[40] Biega, A.J. and Finck,M. (see note 26 above).
[41] Faisal, K., 'Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective.' *Communication Law and Policy*, (2023) 28(1) 67-97.
[42] See Mühlhoff, R., and Ruschemeier, H., 'Updating Purpose Limitation for AI: A normative approach from law and philosophy.'*SSRN* (USA, 11th June 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4711621> accessed 24th April, 2024
[43] Guembe, B., and others, 'The emerging threat of ai-driven cyber-attacks: A review.' *Applied Artificial Intelligence*, (2022) 36(1) 2037254.

providing automated predictions by analyzing large volumes of data and discovering patterns, are the very same features that cybercriminals misuse and abuse for ill gain.[44] Deepfakes, for example, are a popular abuse of AI. Deepfakes involve the use of AI techniques to craft or manipulate audio and visual content to appear authentic. AI systems can also malfunction when exposed to untrustworthy data, and attackers are exploiting these issues. A better illustration is when adversaries deliberately confuse or even "poison" AI systems to make them malfunction through errant markings on the road to mislead a driverless car, potentially making it veer into oncoming traffic. The US National Institute of Standards and Technology stated that currently, there is no foolproof method for protecting AI from misdirection, and AI developers and users should be wary of any who claim otherwise.[45] This indicates the need for robust regulatory frameworks and security measures to safeguard AI systems.

Consent is a data privacy issue in the use of AI as AI systems often collect and use data without obtaining explicit user consent, and when users' rights are disregarded, it results in a breach of trust.[46] In addition, autonomy is a key concern. AI systems often make assumptions about user preferences based on collected data, which can influence the information served to users, potentially limiting their exposure to a diverse range of content.[47] AI can subtly guide human decision-making through recommendation algorithms that shape the choices users make, from the music they listen to, to the products they buy.

With the growing influence of AI, many individuals are worried about the security of their personal data.**48** With AI systems storing and processing vast amounts of sensitive information, the risk of data breaches, hacking, and unauthorized access is indeed a significant concern. This concern is not just theoretical but has manifested in real-world incidents. In 2023, a bug in

[44] Ibid.
[45] National Institute of Standards and Technology, 'NIST Identifies Types of Cyberattacks That Manipulate Behaviour of AI Systems' *NIST.gov* (Washington DC, January 4, 2024) <https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems> accessed 23rd April, 2024.
[46] Andreotta, A. J., Kirkham, N., and Rizzi, M., 'AI, big data, and the future of consent.' *Ai & Society*, (2022) 37(4) 1715-1728.
[47] Laitinen, A. and Sahlgren, O., 'AI Systems and Respect for Human Autonomy' *Frontiers of Artificial Intelligence* (2021) 4 <https://doi.org/10.3389/frai.2021.705164> accessed 22nd April, 2024,
[48] Makridakis, S., 'The Forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms'. *Futures* (2017) 90, 46-60.

ChatGPT's source code resulted in a breach of sensitive data, where unauthorized actors were able to view users' chat history due to a vulnerability in the Redis memory database used by OpenAI.[49] In September 2023, Microsoft AI team accidentally exposed 38TB of corporate data.[50] The availability of AI tools has led to the rise of 'Script Kiddies' - individuals with little to no technical expertise using pre-existing automated tools or scripts to launch cyberattacks.[51] As AI continues to evolve and become more integrated into our daily lives, the importance of safeguarding sensitive data and maintaining user privacy cannot be overstated.

There is a growing apprehension about how companies might use the data they collect. This concern is not unfounded as AI companies are collecting vast amounts of data about their consumers and employees. Concerns range from the sale of personal information to third parties to the utilization of data for targeted advertising or profiling.[52] AI algorithms can be highly complex and difficult to interpret, which makes increases concerns about the opacity of AI decision-making processes and how this might affect privacy of personal information. There are also concerns about how long data are retained by companies and whether companies should be allowed to retain data indefinitely or if there should be limitations on data retention.[53] Privacy concerns also extend to issues of algorithmic bias, where AI systems can perpetuate or exacerbate existing biases in data.[54] This can lead to discrimination in areas such as lending, hiring, and criminal justice.[55]

[49] Markets and Markets, 'Generative AI's first data breach: OpenAI takes corrective action, bug patched.' *Markets and Markets* (USA, September 2023) <https://www.marketsandmarkets.com/industry-news/Generative-AI-Breach-Openai-Takes-Action-Bug-Patched> accessed 26th April, 2024.
[50] Divatia, A., 'Data Security and Responsible AI must be a Top Priority in 2024' *Forbes* (New Jersey, December 15, 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/12/15/data-security-and-responsible-ai-must-be-a-top-priority-in-2024/?sh=5978fb407cc6> accessed 26th April, 2024.
[51] Rech, F., 'The growing threat of data breaches in the age of AI and data privacy' *Techradar Pro* (India, January 24, 2024) <https://www.techradar.com/pro/the-growing-threat-of-data-breaches-in-the-age-of-ai-and-data-privacy> accessed 26th April, 2024.
[52] Ibid, p.40.
[53] See Boyne S., 'Data Protection in the United States' *The American Journal of Comparative Law* (2018) 66(1) 299-343.
[54] See Zhisheng Chen, 'Ethics and discrimination in artificial intelligence-enabled recruitment practices.' *Humanities and Social Social Sciences Communication* (2023) 10, 567 https://doi.org/10.1057/s41599-023-02079-x
[55] Ibid.

High-profile data breaches, such as the Equifax breach in 2017 and the Facebook/Cambridge Analytica scandal in 2016, illustrate the criticality of these concerns and the consequences of inadequate data privacy. The Equifax breach in 2017 was one of the largest data breaches in history, affecting over 147 million people. The company had to pay a $700 million settlement with the Federal Trade Commission and another $425 million settlement with affected individuals. The Analytica scandal involved the harvesting of Facebook data of 87 million people for advertising during elections. Eventually, Facebook had to settle a class-action lawsuit for $650 million. In light of the foregoing, key expectations arise. Customers expect businesses to be transparent about how their data is collected, used, and shared. This includes providing clear privacy policies and easy-to-understand explanations of data practices. Customers also desire control over their personal data. This includes the ability to opt in or out of data collection, as well as the power to update, correct, or delete their data. In the same vein, businesses are expected to invest in security infrastructure and take robust measures to safeguard personal data from breaches and unauthorized access. Customers expect companies to use their data ethically and not exploit such data for purposes that individuals have not consented to. In the event of a data breach, customers expect companies to be accountable for their actions and notify them while promptly taking steps to rectify the situation.

Legal Framework for Personal Data Privacy in the U.S.

With the growing recognition of the importance of personal privacy, the United States boasts of a complex data privacy regulation environment, which is characterised by a combination of federal, state, and sector-specific legislation. Key laws such as the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the General Data Protection Regulation (GDPR) will be examined.

California Consumer Privacy Act (CCPA)

The CCPA serves an extensive data privacy regulatory framework. While initially made to protect the privacy of California residents, this law has become a significant legal blueprint for

governing AI usage of data.[56] This is because it introduces new consumer rights around businesses' use, deletion, withdrawal of, and access to, citizens' personal information. Moreover, the CCPA has broad national and global ramifications given California's prominent and influential position in the global and, in particular, digital economy.[57]The CCPA grants individuals right over their personal data, and how such data is acquired, handled and distributed by entities or companies. It establishes the general duties of businesses that collect personal information, including the obligation to inform consumers about their rights, the categories of personal information collected, and the purpose of data processing.[58]

With the increasing deployment of AI for data analysis and processing, businesses are obligated to be transparent about how AI is employed in data collection and processing to ensure compliance with CCPA requirements. For businesses using AI for customer profiling and data analysis, Section 1798.105 is particularly relevant. It provides thus:

> (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.
>
> (b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.
>
> (c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

AI-driven systems that process personal data must enable consumers to request the deletion of their data, ensuring compliance with CCPA's right to be forgotten. Section 1798.115 gives consumers the right to know if their data is being sold or shared and to whom. It provides that:

---

[56] Paka, A., 'How Does the CCPA Impact Your AI' *Forbes* (New Jersey, February 20, 2020). <https://www.forbes.com/sites/forbestechcouncil/2020/02/20/how-does-the-ccpa-impact-your-ai/?sh=2adc68e243c7> accessed 25th April, 2024.
[57] Ibid.
[58] Section 1798.100 of the CCPA.

> (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer…

This provision has implications for profiling and data analysis. The CCPA mandates a high degree of transparency about data collection and usage, meaning that businesses must clearly inform consumers about how their data is being used for profiling or data analysis. Consumers also have the right to opt out of their data being sold, which could limit the scope of data available for profiling and analysis. The CCPA encourages data minimization, i.e., collecting only the data that is necessary for the specified purpose, impacting the breadth and depth of profiling and data analysis activities1. Also, the right to delete under section 1798.105, means that businesses may need to remove consumer data from their datasets used for profiling and data analysis.

AI systems may sometimes generate inaccuracies in personal data processing. Section 1798.106 allows consumers to correct inaccuracies in AI-driven data systems. Also, for businesses using AI for personalized advertising and customer profiling, section 1798.120 gives consumers the right to opt out of the sale or sharing of their data processed through AI systems. Furthermore, section 1798.121 allows consumers to limit the use and disclosure of their personal information. More importantly, Section 1798.125 safeguards consumers against any adverse actions by businesses in response to their data privacy choices. It ensures that businesses cannot retaliate or discriminate against consumers who exercise their data privacy rights. Practically, a consumer who opts out of data selling, for instance, cannot be denied services or charged different prices. This provision upholds the principle of consumer sovereignty in data privacy. Section 1798.130 further sets out obligations for businesses regarding notice, disclosure, correction, and deletion of consumer personal data. It mandates that businesses provide clear notice to consumers about their data collection practices, disclose specific pieces of collected personal information upon request, correct inaccurate personal information, and delete personal information upon the consumer's request. The significance of this provision is that it enforces transparency and

accountability in businesses' data practices, thereby empowering consumers to make informed decisions about their data.

While the CCPA enhances data privacy, there are certain lapses in safeguarding personal information in the context of AI use. First, the law is challenging to enforce, particularly for individuals with limited resources.[59] This means that while the law provides a framework for data privacy, the practical implementation of these regulations is difficult as a result of the complexity of data practices, the resources required for enforcement, and the need for businesses to adapt their operations to comply.[60] While the CCPA allows consumers to sue for data breaches, the practicality of such legal actions and the resulting compliance is uncertain. The primary enforcer of the law is the California attorney general, who is expected to bring only a limited number of cases annually, rendering the CCPA somewhat toothless in terms of enforcement. In other words, difficulties arise when pursuing legal action, in the aspect of the costs involved, the complexity of proving a violation, and the uncertainty of whether businesses will comply with any resulting court orders.[61] Second, the absence of the private right of action, which was initially intended to permit individuals to sue companies for law violations, further diminishes the law's impact due to concessions made during the legislative process to accommodate lobbying interests. Notably, these interests aim to limit privacy provisions and push back against future privacy legislation. Third, the CCPA falls short of setting a more robust standard for data collection practices by requiring consumers to opt out of data collection and monetization, rather than demanding companies to obtain explicit consent for data collection without the option to refuse services. This opt-out approach is unlikely to lead to significant change, as it relies on consumers to take proactive steps to protect their rights, which many may not do.

---

[59] Zappa J., 'The California Consumer Privacy Act' Promise and Limitations'*Streetfight* (California, 6 January, 2020) <https://streetfightmag.com/2020/01/06/the-california-consumer-privacy-acts-promise-and-limitations/#:~:text=Major%20weaknesses%20include%20the%20law's,companies%20have%20collected%20about%20them.> accessed 03 November, 2023.

[60] Abernethy, D., 'Top-10 takeaways from the California AG's CCPA enforcement case examples'*IAPP* (New Haven, September 1, 2021) <https://iapp.org/news/a/top-10-takeaways-from-the-california-ags-ccpa-enforcement-case-examples/> accessed 26th April, 2023.

[61] See Abernethy, D., (note 61 above). Also see Valdetero, J.M. and Zeetony, D.A., 'CCPA Litigation Up 44.1%' *The National Law Review* (2022) 14(121) <https://natlawreview.com/article/ccpa-litigation-441> 27th April, 2024.

Fair Credit Reporting Act (FCRA)

The FCRA regulates the collection, use, and dissemination of consumer credit information in the United States. AI is a fundamental component of modern e-commerce platforms, powering personalised recommendations, credit decisions, and targeted advertising. The FCRA imposes requirements and safeguards to ensure the fair and ethical use of AI in e-commerce.

E-commerce platforms often rely on consumer data for various purposes, such as determining eligibility for credit to provide personalised product recommendations and set prices. Section 604 of the FCRA establishes permissible purposes for accessing consumer reports. By implication, there must be a legal basis for using AI systems to make credit or eligibility decisions. Section 607 essentially stipulates that ecommerce platforms should have rigorous compliance procedures, especially when AI algorithms are involved. Moreover, in order to ensure transparency and trust, consumers have the right to access the data used in AI decision-making.[62]

Disputes regarding data accuracy are common in AI-driven e-commerce. Section 611 of the FCRA sets out procedures for handling such disputes. Noncompliance with FCRA regulations can result in civil liability for these platforms, both for wilful and negligent violations.[63] Given the sensitive nature of the information processed by AI systems, proper disposal of records is salient to data security and privacy.[64] Section 628 provides that e-commerce platforms must ensure that they dispose of consumer data securely.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The HIPPA was enacted with the aim of regulating issues related to health care access, fraud prevention, administrative simplification, and tax-related health provisions in the US. HIPAA has particular relevance as it governs the handling of protected health information (PHI) and plays a vital role in ensuring the privacy and security of healthcare data. It sets strict standards

[62] See section 609.
[63] See sections 616 and 617.
[64] Mudorch B., 'Privacy and artificial intelligence: challenges for protecting health information in a new era' *BMC Med Ethics* (2021) 22 (122), 3.

for protecting the privacy and security of patient data. Healthcare organizations, both covered entities and business associates, have obligations under the HIPPA.

Unregulated or under-regulated use of AI in healthcare could lead to healthcare fraud and abuse, which may have data security implications. HIPAA requires healthcare entities to take certain measures under sections 701-707 to safeguard PHI from unauthorized access, which is crucial in the context of AI systems handling healthcare data. AI applications in healthcare, such as diagnostic tools or patient record management, must comply with HIPAA's privacy and security rules to protect patient information.

The HIPAA Privacy Rule (Title II, Subtitle F) sets standards for the use and disclosure of PHI. Any AI applications that access, use, or disclose PHI must adhere to these rules. Entities using AI systems need to ensure patient data privacy by limiting access to authorized personnel and purposes, obtaining patient consent where required, and maintaining audit trails of data access.

Sections 351 to 357 of HIPAA mandate security standards for electronic PHI (ePHI). AI systems that handle ePHI, such as electronic health records (EHR) or AI diagnostic tools, must implement safeguards like access controls, encryption, and data backups to protect patient information from breaches and cyberattacks. In cases of negligence with data handling, HIPAA provides for civil and criminal penalties for non-compliance with its privacy and security provisions. If AI systems fail to secure or use PHI appropriately, concerned entities or institutions can face substantial fines and legal consequences. Moreover, the HIPAA emphasizes the importance of standardized transactions and data interchange in healthcare. AI applications that utilize health data need to adhere to these standards to ensure interoperability and data privacy. Compliance with these standards simplifies data sharing between AI systems and healthcare providers.

Data sharing and collaboration between healthcare entities and AI developers is common. HIPAA ensures that when healthcare organizations share patient data with AI vendors or research institutions, they do so in a manner compliant with privacy and security regulations.[65]

[65] Kim Theodos and Scott Sittig, 'Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply' *Perspectives in Health Information Management* (2021) 18(1) 11.

Research that involves AI and patient data, whether for treatment or diagnostics, must comply with HIPAA requirements for obtaining patient consent for research, de-identifying data to protect privacy, and following strict rules regarding data access and disclosure. Similarly, AI applications that operate within EHR systems must adhere to HIPAA's privacy and security rules to ensure the confidentiality of patient records and related data.[66]

General Data Protection Regulation (GDPR)

The GDPR is an EU legislation and not a U.S. law. Notwithstanding, the GDPR influences American businesses that operate globally.[67] It sets standards for data protection and privacy, including the right to erasure, data portability, and transparent data processing. U.S. companies processing the data of European citizens must ensure compliance with the GDPR's provisions.

Under Article 5, the GDPR establishes fundamental principles for processing personal data - lawfulness, fairness, and transparency. In the USA, companies using AI for various purposes, not limited to e-commerce, have a duty to ensure that data processing aligns with these principles. AI systems that process personal data, such as those used for targeted advertising, product recommendations, or even healthcare diagnostics, need to comply with these fundamental principles to safeguard individuals' privacy and rights.

Article 6 of the GDPR provides several lawful bases for data processing. This includes obtaining user consent, fulfilling contractual obligations, and pursuing legitimate interests. When AI is employed, companies must carefully consider and document the lawful bases for processing personal data. For example, in the case of AI-driven personalized advertising or recommendation systems, e-commerce companies are to ensure that their data processing activities are in compliance with these lawful bases.

Article 12 of the GDPR imposes an obligation to provide clear and transparent information to users regarding how their data is processed. Transparency is germane to ensure users understand

[66] McGraw S. and Mandl K., 'Privacy Protections to Encourage Use of Health-Relevant Digital Data in a Learning Health System' *NPJ Digital Medicine* (2021) 4(2) 2.
[67] Martin N., and others, 'How Data Protection Regulation Affects Startup Innovation' *Information systems frontiers* (2019) 21, 1307-1324.

how their data is utilized to make informed decisions.[68] Additionally, individuals have the right to request access to their personal data processed by AI systems. This right to data access is crucial, as it empowers individuals to maintain control over their data and understand how AI technologies impact their privacy.

By implication of the GDPR, businesses that employ AI systems are data controllers. As data controllers, article 24 states that they have a responsibility to ensure GDPR compliance throughout their data processing activities, regardless of whether AI is involved. The GDPR also enables data subjects to lodge complaints with supervisory authorities if they believe their data rights have been violated. Therefore, businesses or organizations using AI must be prepared to address user concerns and regulatory inquiries effectively. Furthermore, under article 82, if a data subject suffers damage due to a GDPR violation involving AI systems, they are entitled to compensation. While federal proposals have been introduced, achieving consensus on such laws remains a challenge. This aspect is a strong incentive for organizations to invest in robust privacy protection measures when deploying AI.

Challenges from Regulatory Gaps

There is a growing concern about how the rapid evolution of AI technology poses a significant challenge to existing legal and regulatory frameworks.[69] The exponential growth of AI, which is currently driven by disruptive models like ChatGPT and GPT-4, has expedited the integration of AI across multiple industries and sparked an unprecedented technological competition amongst major players in the tech market. The swift advancement has outpaced the knowledge of the legislature and jurisdictional limits of the federal courts.[70]The static nature of current regulations struggles to keep pace with the speed of innovation in AI.[71] As examined in the previous section,

[68] Yu L. and Li Y., 'Artificial Intelligence Decision-Making Transparency and Employees' Trust: The Parallel Multiple Mediating Effect of Effectiveness and Discomfort" *Behav Sci (Basel)* (2022) 12, 127.
[69] Dwivedi, Y. and others., 'Evolution of artificial intelligence research in Technological Forecasting and Social Change: Research topics, trends, and future directions' *Technological Forecasting and Social Change* (2023) 192 122579.
[70] Coeckelbergh M., 'Artificial intelligence: some ethical issues and regulatory challenges,' *Technology and Regulation* (2019) 31.
[71] Kingston J., 'Using artificial intelligence to support compliance with the general data protection regulation,' *Artificial Intelligence and Law* (2017) 25(4) 429.

the CCPA for instance is limited in its potency to safeguard data privacy in light of AI. Its enforcement is challenging, particularly for individuals with limited resources. The absence of a private right of action further diminishes its impact. Moreover, the CCPA requires consumers to opt out of data collection and monetization, rather than demanding companies to obtain explicit consent for data collection. The FCRA, on the other hand, mandates rigorous compliance procedures, especially when AI algorithms are involved. However, does not provide specific guidelines for AI use, which could lead to inconsistent interpretations and applications of the law. The HIPAA also does not specifically address the unique challenges posed by AI, such as the potential for AI algorithms to infer sensitive information from non-sensitive data.

The call for government intervention in regulating AI activities within corporate spheres is increasingly resonant.[72] Influential figures in the domain of AI such as Sam Altman, CEO of OpenAI, have advocated for the establishment of a new agency to license and ensure compliance with safety standards for AI endeavors.[73] Similarly, Brad Smith, President of Microsoft, aligning with this sentiment, emphasized the need for swifter governmental action and highlighted the proactive role that the government must play in this swiftly evolving landscape.[74] These clamors indicate the exigency perceived within the AI industry about how the under-regulation of AI poses unprecedented risks to data privacy and security of personal information especially.

However, the practical implementation of such regulatory measures encounters serious challenges. Recent discussions and debates surrounding the development and regulation of AI indicate how difficult it is to make the shift from theoretical talks about AI regulation to actual implementation.[75] For instance, despite the initial endorsement of regulatory initiatives, subsequent conflicting statements emerged from industry leaders regarding compliance with proposed regulations on AI.[76] Such complexities have surfaced amid discussions between AI leaders and regulatory bodies, such as the European Union, where concerns regarding privacy

[72] Feretti T., 'An institutionalist approach to AI ethics: justifying the priority of government regulation over self-regulation' *Moral Philosophy and Politics* (2022) 9(2) 239.
[73] LaGrandeur K., 'How safe is our reliance on AI, and should we regulate it?' *AI and Ethics* (2021) 1 93.
[74] Ayanna Howard, 'The Regulation of AI-Should Organizations Be Worried?' *MIT Sloan Management Review* (2019) 60(4) 3.
[75] Wheeler T., 'The three challenges of AI regulation' *Brookings* (USA, June 15 2023). <https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/> accessed 20th November, 2023.
[76] Ibid.

rules have affected the deployment of AI products in certain geographical areas.[77] This backdrop demonstrates that, in addition to regulatory measures, a sophisticated grasp of the rapidly changing technological landscape is necessary to keep up with the advancement of AI.

Determining the scope of regulatory intervention is also critical. This requires evaluating the risk profiles of diverse AI applications, ranging from conventional digital abuses like consumer scams and discrimination to emerging digital threats amplified by AI's expansive capabilities.[78] Treleavan and Batrinca posited that the challenge with this approach is in differentiating regulations according to the level of risk posed by varying AI applications, necessitating a risk-based strategy for focused and efficient regulation.[79]

In response to the increasing privacy concerns on the rapid growth in AI use, there has been a call for federal legislation to create a unified privacy framework across all states and avoid a patchwork of regulations.[80] The balance between ensuring individual privacy and facilitating business innovation remains an ongoing process. One of the primary challenges in the context of AI and personal data protection is reconciling the rapid advancements in AI with existing legal frameworks.

Many of the current laws were not designed with AI in mind, and they may not address the specific ways AI systems collect, process, and use personal data. AI technologies, such as machine learning and deep learning, often require access to substantial datasets, including personal information, to operate effectively.[81] This raises questions about how data is collected, used, and stored, and whether it complies with existing regulations.[82] Additionally, retaining user data for extended periods can enhance the effectiveness of AI algorithms, but it also heightens privacy risks, as data breaches become more damaging over time.

---

[77] Ibid.
[78] Truby J., Brown R., and Dahdal A., 'Banking on AI: mandating a proactive approach to AI regulation in the financial sector,' *Law and Financial Markets Review* (2020) 14(2) 110.
[79] Treleaven P. and Batrinca B., 'Algorithmic regulation: automating financial compliance monitoring and regulation using AI and blockchain,' *Journal of Financial Transformation* (2017) 45 14.
[80] Kerry C., 'How privacy legislation can help address AI' *Brookings* (USA, 7 July, 2023) <https://www.brookings.edu/articles/how-privacy-legislation-can-help-address-ai/> accessed 5 November, 2023.
[81] Murdoch B., 'Privacy and artificial intelligence: challenges for protecting health information in a new era.' *BMC Med Ethics* (2021) 22(122) <https://doi.org/10.1186/s12910-021-00687-3> accessed 6th November, 2023.
[82] Ibid.

The implementation of AI systems also introduces complexities in data anonymization and consent management. For instance, anonymizing data to the level required by privacy laws can be challenging, particularly with advanced AI techniques. Moreover, AI systems that continuously learn from data may operate in ways that challenge traditional consent models, where users might not have granular control over data usage.[83] Moreover, AI systems, when used in data-driven applications, can inadvertently introduce biases and ethical concerns into data processing.[84] These biases may lead to discriminatory outcomes and privacy breaches, as they can affect how personal data is collected, processed, and used. Biases could result in unfair or unequal treatment of individuals and impact their data privacy and protection.

Findings of the Paper

The paper finds that the rapid evolution of AI technology poses significant challenges to existing legal and regulatory frameworks. The swift advancement of AI, driven by disruptive models like ChatGPT and GPT-4, has outpaced the knowledge of the legislature and jurisdictional limits of the federal courts. The static nature of current regulations struggles to keep pace with the speed of innovation in AI. Existing laws such as the CCPA, FCRA, and HIPAA have limitations in safeguarding data privacy in light of AI. Their enforcement is challenging, particularly for individuals with limited resources. The absence of a private right of action further diminishes their impact. Moreover, these laws require consumers to opt out of data collection and monetization, rather than demanding companies to obtain explicit consent for data collection.

Calls for government intervention in regulating AI activities within corporate spheres are increasingly resonant. Influential figures in the domain of AI have advocated for the establishment of a new agency to license and ensure compliance with safety standards for AI endeavors. However, the practical implementation of such regulatory measures encounters serious challenges.

Determining the scope of regulatory intervention is also critical. This requires evaluating the risk profiles of diverse AI applications, ranging from conventional digital abuses like consumer

[83] Ibid.
[84] Belenguer L., 'AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry' *AI Ethics* (2022) 2 771.

scams and discrimination to emerging digital threats amplified by AI's expansive capabilities. In response to the increasing privacy concerns on the rapid growth in AI use, there has been a call for federal legislation to create a unified privacy framework across all states and avoid a patchwork of regulations. The balance between ensuring individual privacy and facilitating business innovation remains an ongoing process.

Many of the current laws were not designed with AI in mind, and they do not address the specific ways AI systems collect, process, and use personal data. The implementation of AI systems also introduces complexities in data anonymization and consent management. Moreover, AI systems, when used in data-driven applications, can inadvertently introduce biases and ethical concerns into data processing. These biases may lead to discriminatory outcomes and privacy breaches, impacting individuals' data privacy and protection.

In light of these findings, a sophisticated grasp of the rapidly changing technological landscape is necessary to keep up with the advancement of AI and ensure the protection of personal data privacy.

Recommendations for Balancing Consumer Convenience with Privacy

The integration of AI in business operations often leads to tensions between delivering AI-driven convenience and ensuring robust privacy compliance. Achieving a balance between AI-driven convenience and privacy compliance necessitates strategic considerations. Foremost, incorporating privacy considerations from the outset when designing AI systems is a best practice. This involves minimizing data collection to what is strictly necessary to deliver specific services in order to ensure data security and reduce privacy risks. Granting users control over their data is essential. Providing clear options for data deletion, opting out of data collection, and managing data settings gives users more control over their personal data.[85] Prioritisation of transparency and obtaining clear user consent is a proactive approach for businesses to balance the use of AI with personal data protection while fostering trust and ensuring privacy

[85] Kerry C., see note 36.

compliance. In the same vein, recognizing that user preferences may change over time, businesses should allow users to revisit and modify their consent settings at any time. This dynamic consent model accommodates changing user expectations and preferences in line with the GDPR and the CCPA.

Also, periodic audits and compliance checks can ensure that AI systems align with privacy regulations and best practices. It allows businesses to adapt to evolving privacy standards. Similarly, AI systems are capable of processing and analysing vast amounts of data with incredible speed and sophistication. Legal frameworks need to catch up by defining the scope of permissible data use and considering issues of consent, data minimization, and storage limitations.

Legal professionals play a crucial role in addressing the complex landscape of AI and data protection challenges. They are often responsible for interpreting and applying existing privacy laws and regulations to AI-related activities. They provide guidance on how organizations can remain compliant while harnessing the power of AI. Legal professionals assess the legal risks associated with AI initiatives, especially those involving personal data, and advise how an organization collects, uses, and protects data In light of the increasing danger of AI to data protection and privacy, legal professionals, working in-house for businesses that adopt AI, need to be proactive in crafting privacy policies that must be easily understood by consumers and aligned with relevant regulations, while specifying data handling requirements, responsibilities, and liabilities. Legal experts must collaborate closely with AI developers, data scientists, and cybersecurity professionals to understand the technical intricacies of AI systems.

More importantly, the pace at which AI technologies advance challenges the static nature of current laws and regulations.[86] A key recommendation would be to establish regulatory frameworks that are not only robust but also adaptive. This means creating regulatory frameworks that can evolve alongside technological innovations. It is therefore imperative to encourage continuous dialogue between regulatory bodies, industry stakeholders, and technological experts, allowing for the identification of emerging challenges and ensuring that

[86] Treleaven P. and Batrinca, B., op cit., 18.

regulations remain relevant and effective in safeguarding consumer rights while enabling technological progress.[87] Moreover, enabling partnerships between governments, academic institutions, and industry players can contribute to establishing international benchmarks for AI regulation, thereby fostering a harmonized global framework that upholds ethical standards and protects consumer rights universally. This adaptability hinges on a proactive approach from regulatory authorities, where they anticipate future developments in AI and preemptively draft flexible guidelines capable of addressing unforeseen challenges.

Lastly, international collaboration is essential in shaping cohesive and globally applicable AI regulations. The creation of uniform AI standards and guidelines can be facilitated by promoting cross-border cooperation among regulatory authorities. This involves engaging in dialogue and sharing best practices across nations to establish a unified approach to AI governance. Standardizing principles regarding data protection, algorithmic transparency, and ethical AI practices across jurisdictions reduces confusion and provides a unified set of expectations for businesses operating in multiple countries.[88]

Conclusion

The integration of AI into personal data protection presents an array of challenges and opportunities. Undoubtedly, the pace of AI evolution has outstripped the stride of existing data privacy laws, thereby creating a palpable gap in regulatory frameworks.[89] On one hand, AI offers remarkable capabilities for enhancing customer convenience, personalization, and operational efficiency.[90] On the other hand, it raises critical challenges related to privacy, transparency,

[87] Yara O. and others, ., 'Legal regulation of the use of artificial intelligence: Problems and development prospects,' *European Journal of Sustainable Development* (2021) 10(1) 281.
[88] See Aho B. and Duffield R., 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China,' *Economy and Society* (2020) 49(2) 187.
[89] Meskó B, and Topol E.J., 'The imperative for regulatory oversight of large language models (or generative AI) in healthcare,' *Digital Medicine* (2023) 6(1) 120.
[90] Bawack R. and others, 'Artificial intelligence in E-Commerce: a bibliometric study and literature review' *Electron Markets* (2022) 32, 297.

fairness, and security.[91] In the light of rapid growth of AI, achieving a delicate balance between customer convenience and privacy compliance is more important. Businesses that successfully navigate this balance can deliver personalized, convenient services while maintaining the trust and loyalty of their customers.[92] This balance is not only an ethical imperative but also a competitive advantage in the digital era. In essence, the recommendations proposed in this paper will help to fortify regulatory adaptability and bridge the wide gap between existing frameworks and AI development in order to ensure adequate personal data protection while improving consumer convenience and overall user experience.

[91] Perifanis, N. and Kitsios F., 'Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review' *Information* (2023) 14(2) 85.

[92] Schäfer F., and others., 'Data-driven business and data privacy: Challenges and measures for product-based companies,' *Business Horizons* (2023) 66(4) 493.