Int. j. adv. multidisc. res. stud. 2025; 5(5):467-472

Received: 28-07-2025
Accepted: 08-09-2025

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Personalization vs. Privacy: Consumer Trust in AI-Driven Banking Marketing

[1] Adeleke Sulaimon Adepeju, [2] Chidimma Augustina Edeze, [3] Micheal Tokunbo Adenibuyan

[1] Independent Researcher, Lagos, Nigeria
[2] Nile University of Nigeria, Nigeria
[3] Bells University of Technology, Nigeria

Corresponding Author: **Adeleke Sulaimon Adepeju**

Abstract

Artificial intelligence (AI) has transformed the banking sector, enabling highly personalized marketing strategies that improve customer engagement and business performance. AI allows banks to provide tailored credit, loan, and investment products by analyzing financial behavior. While personalization enhances customer satisfaction and loyalty, it simultaneously raises critical concerns about privacy, transparency, and trust. Sensitive financial data, opaque algorithms, and aggressive targeting create risks of consumer discomfort, regulatory penalties, and reputational damage. Frameworks such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) provide a foundation for safeguarding consumer rights, emphasizing transparency, consent, and accountability. This paper argues that personalization and privacy must be treated as interdependent rather than competing priorities. Banks that integrate transparency, consent-driven data practices, and explainable AI into their marketing strategies can balance innovation with responsibility, positioning privacy not as a regulatory hurdle but as a competitive advantage in fostering consumer trust.

Keywords: Artificial Intelligence, Banking Marketing, Personalization, Privacy, Consumer Trust, GDPR, CCPA, Explainable AI

Introduction

In recent years, artificial intelligence (AI) has transformed the financial services sector, reshaping how banks interact with consumers and deliver value. One of the substantial applications of Artificial Intelligence has been on marketing. The aim has been to leverage machine learning algorithms in analyzing customer data. Therefore, it is possible to create customized products, provide targeted offers, and predict insights on customer behavior. Instead of focusing more on generic advertisements, modern banking customers might receive a customized credit card promotion, which will be determined by their spending habits. Moreso, it is possible to have mortgage refinancing options that are in line with life changes of an individual or create an investment opportunity that is based on a client's risk profile. The application of Artificial Intelligence marketing is promising not only in enhancing customer engagement but also in promoting efficiency and profits within financial institutions.

However, the progress in technology raises several vital issues. For instance, there is an increasing tension between customization and privacy. Consumers tend to appreciate banks when they anticipate their personal needs and offer solutions that are unique to their financial goals. The personalization in most instances creates loyalty, trust, and satisfaction. The reason is that customers tend to feel understood and valued within the financial institution. Alternatively, the use of sensitive fiscal and behavioural data for marketing raises significant concerns (Arrieta, 2020) [2]. Most customers end up being scared that the use of such personalized information might escalate into surveillance, manipulation, and exploitation. There are reported incidents of high-profile data breaches, unauthorized sharing of personal information that is unauthorized, and the use of opaque algorithms to support decision-making. They all play a key role in heightening anxiety. Therefore, while personalization might depict solid gains, it simultaneously increases the risk of eroding consumers' trust, especially if privacy has been compromised.

The regulatory landscape has responded decisively to these concerns. The two primary frameworks that are influential in nature include the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). The two have been specifically designed to recover control of personal information for people and boost aspects of accountability in organizations that oversee the processing of customer data (Mu & Liu, 2024) [5]. GDPR was implemented in 2018, and its main obligation is to set stringent requirements pertaining to issues of consent, transparency, and the right of individuals to access, correct, and erase their information. Additionally, it presents a significant penalty to institutions that fail to abide therefore, terming it a global benchmark for data protection (Arrieta, 2020) [2]. CCPA, on the other hand, was enacted in 2020, and its main contribution is to grant Californians the right to be aware of what personal information is being gathered from them, request a deletion, if need be, and opt out of the sale or sharing. There is a thin line of distinction between GDPR and CCPA, but they both showcase a growing movement within the United States towards solidifying consumer data rights.

For the financial institutions that are capitalizing on Artificial Intelligence, the regulations might not be granted priority but remain important in making strategic and operational decisions. It is not possible to have personalization in the absence of privacy. Personalization and privacy are intertwined, and they both contribute to shaping consumer trust. If there is compliance with GDPR and CCPA, the motive should not be solely on avoiding fines (Mu & Liu, 2024) [5]. Instead, attention needs to be directed towards ensuring the customers feel secure by being aware that the data collected from them is being respected and managed responsibly. Establishing the right balance between innovation and regulation is a defining problem among most modern banking institutions.

The paper explores the complex interplay between personalization and privacy in AI-driven banking marketing, with a particular focus on how consumer trust is affected. A key argument presented is that while AI provides a powerful tool useful in enhancing customer engagement, the gains can only be sustainable if banks are in a better position to embrace transparency, consent-driven activities, and ethical data management that is in line with the guidelines provided in GDPR and CCPA. In the end, trust among customers will determine the success of using Artificial Intelligence marketing incentives, prioritizing privacy personalization not just as a regulatory need but as a competitive advantage in the digital marketing era.

The Promise of Personalization

Artificial intelligence has redefined how banks understand and engage with their customers, moving beyond broad demographic targeting to individualized financial experiences. The power of Artificial Intelligence exists in its potential to assess large amounts of structured and unstructured information ranging from transaction histories to credit usage (Gyau *et al*., 2024) [3]. If the application and implementation take place ethically and strategically, the data-driven approach grants the bank the opportunity to render high-quality services that are in line with the needs of customers.

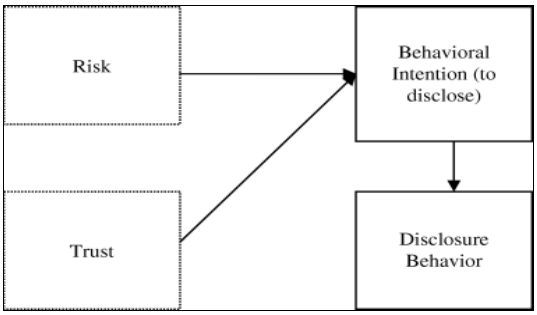

Fig 1: The Privacy Paradox

Customer Experience

From a consumer's point of view, convenience and relevance are the two primary compelling gains associated with personalization. For instance, Artificial Intelligence systems can be used to monitor rent payments that are recurrent in nature. In the process, it becomes possible to proactively suggest strong mortgage commodities that will meet consumers' needs once they showcase long-term financial stability (Abdulsalam & Tajudeen, 2024) [1]. Also, if there is an assessment of saving behaviours, banks are better positioned to recommend investment portfolios that have been customized to meet the personal risk preferences. Customized offers are important since they reduce cognitive load on consumers of the different products. Their scope reduces from a wide array of generic products to those that specifically apply to their situation. Therefore, it becomes possible to have meaningful solutions in place that are aligned with individual financial needs (Mu & Liu, 2024) [5]. The interactions are equally relevant since they enhance customer satisfaction by depicting banking operations as less transactional and more advisory. Since attention is directed towards customer experience, AI-driven personalization guarantees a shift towards relationship banking where financial institutions operate, and trusted partners as opposed to service providers that are impersonal.

Business Value

For financial institutions, the benefits of personalization extend far beyond improved customer satisfaction. There is targeted marketing, which contributed towards increasing conversion rates, especially when compared to mass-marketing campaigns. The offers resonate more if they have been designed to meet the unique needs of customers. Products that have been personalized in the banking sector can increase sales by up to 20% (Zungu *et al*., 2025) [9]. Nevertheless, they play a key role in fostering long-term loyalty and reducing cases of churn. Artificial Intelligence provides banks with the power to optimize their marketing expenditure. They can focus more on allocating the scarce resources towards serving the needs of different clients who are more likely to engage with specific available offers. In both the short and long run, it becomes possible to increase efficiency. Other than the immediate sales, personalization plays a substantial role in solidifying customers' long-term values based on the existing relationships. For the clients who feel heard and understood, they are more likely to expand on their portfolio of services with the same bank (Khan *et al*., 2025) [4]. For instance, they might shift from checking accounts to loans, credit cards, and even

investment products. Since there is stiff competition in the market where fintech companies operate and the digital banking implementation and adoption are intensifying, personalization is the main distinction that can drive the sustainability towards growth.

Consumer Expectations

Importantly, personalization is not only a business strategy but also a consumer demand. Most customers, especially the young generation, prefer to engage with experiences that have been tailored rather than general interactions. According to research by Yusuff (2024) [8], 91% of customers have a huge tendency to engage with brands that offer services and recommendations that are relevant to their needs. In the banking sector, the outcome depicts higher levels of satisfaction. The reason is that clients end up feeling that the financial institution knows who they are and anticipates that their needs to be addressed. However, there is a vital caveat where personalization will only be adopted if it respects the consumers' boundaries and avoids any instances of intrusiveness. Customers are, on most occasions, in need of services that are useful and not manipulative (Abdulsalam & Tajudeen, 2024) [1]. They are more likely to appreciate options that arise naturally depending on their financial behaviours. If personalization appears to be a surveillance and it leverages sensitive information in a way that they did not anticipate, there will be resistance and revolt. Ultimately, personalization will be successful only if it manages to strike the needed balance of being relevant without invading personal data.

The Privacy Dilemma

The benefits of AI-driven personalization are evident in the banking sector. However, there are a lot of challenges arising from data privacy issues. The same algorithm that is being used to render customized feedback based on sensitive financial and behavioral information fosters a dilemma for customers and the different institutions (Abdulsalam & Tajudeen, 2024) [1]. Amid the dilemma, there is a privacy paradox. Customers need encounters that are seamless and relevant but are still sceptical about how data collection takes place, the approach being used for processing, and designs for sharing (Arrieta, 2020) [2]. If not handled properly, the tension might undermine the trust that customers have placed in the financial institution, therefore exposing banks to serious regulatory and reputational risks.

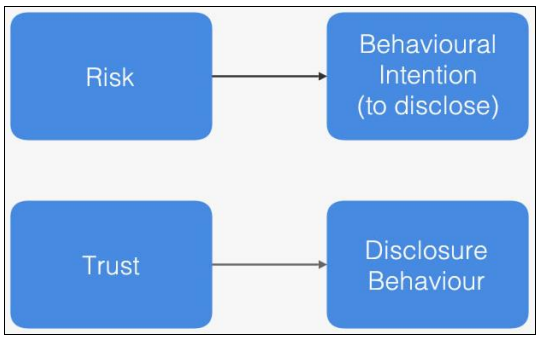

Fig 2: Privacy Dilemma in Increased Conversion

Data Concerns

Financial information is one of the most sensitive parts of personal information. If misused, there will be pronounced negative effects. Customers are in constant worry that gathering transaction history details, location of data, and spending behaviours puts them at risk of fraudulent activities, identity theft, and profiling that is not authorized (Yusuff, 2024) [8]. There are those who are uncomfortable because Artificial Intelligence Systems might be opaque. In most instances, they are described as “black boxes.” In instances where customer do not understand clearly why they are the target audience of unique offers, suspicion rates increase that their personal data is being exploited or used in the absence of their consent. Limited clarity also contributed to a sense of lost control, which has direct effects on limiting customer trust when using digital financial services.

Trust Erosion

Other than the technical issues of data breaches, there is a psychological domain associated with privacy. Personalization that appears to be aggressive in nature can contribute to increased levels of discomfort. A key example is an offer that references highly specific financial behaviours that are intimate. In most instances, they are referred to as “creepy banking.” There are customers who are going to appreciate general investment options, but uneasiness kicks in if there are proactive comments from the bank on recent divorce settlements or frequent medical expenditures (Zungu *et al*., 2025) [9]. The overreach undermines the forecasted gains of personalization by creating a perception of surveillance among the customer as opposed to support. Trust that has been eroded leads to disengagement. Customers will reduce their digital interaction or even opt to shift providers while seeking a financial institution that respects their boundaries.

Regulatory Pressure

In response to the arising concerns, governments have created regulatory actions that are comprehensive and effective in dealing with the different problems. They include the European Union’s General Data Protection Regulation (GDPR) and California’s Consumer Privacy Act (CCPA). The aims of the frameworks are to institute transparency, foster the provision of explicit consent, and accountability among financial institutions while using customer data. A huge responsibility has been placed on banks. If there is non-compliance, stringent penalties are applicable. For example, failing to abide by a provision in the GDPR attracts a penalty of up to €20 million or 4% of global annual revenue (Khan *et al*., 2025) [4]. Moreover, there will be reputational damage that might far surpass the financial obligation. For most institutions, issues do not only arise when trying to adhere to the legal requirements. Instead, problems come from including privacy principles into their different business models in a manner that reinforces rather than undermines personalized efforts.

Table 1: Expanded Key Dimensions of the Privacy Dilemma in AI-Driven Banking Marketing

Dimension	Consumer Perspective	Institutional Risk	Implications for Trust
Data Concerns	Fear of misuse, breaches, or sharing of sensitive financial data without consent.	Legal liability in case of data breaches, costly security investments.	Lack of transparency fuels suspicion and reduces willingness to engage digitally.
Opaque AI Systems	Limited understanding of how algorithms use personal data for targeting.	Difficulty explaining AI decisions to regulators and customers.	Perception of being manipulated damages trust and discourages adoption.
Aggressive Targeting	Overly specific or invasive marketing feels manipulative ("creepy banking").	Customer pushback, reduced engagement, reputational backlash.	Erodes trust by replacing personalization with perceptions of surveillance.
Regulatory Pressure	Expectation that banks comply with GDPR, CCPA, and similar laws to safeguard privacy.	Heavy fines, sanctions, and reputational harm for non-compliance.	Compliance is essential for restoring and maintaining consumer confidence.
Third-Party Sharing	Anxiety about banks selling or sharing data with external advertisers or fintechs.	Breach of customer agreements, legal action, potential restrictions from regulators.	Trust declines sharply if customers perceive exploitation for profit.
Data Accuracy	Concern that outdated or incorrect data leads to irrelevant or unfair targeting.	Biased recommendations, customer dissatisfaction, possible regulatory complaints.	Customers lose faith in both personalization and bank competence if inaccuracies persist.
Security Vulnerabilities	Fear of hacking or unauthorized access to sensitive personal and financial data.	Financial losses, lawsuits, mandatory disclosures, and costly remediation.	Trust collapses when customers believe their financial data is unsafe.
Consent Management	Desire for clear control over what data is collected and how it is used.	Complex systems needed to manage opt-ins/opt-outs and preferences in real time.	Transparency and control enhance trust; absence of consent erodes it.
Cross-Border Data Use	Worry about data being transferred to jurisdictions with weaker privacy protections.	Conflict with GDPR data localization rules; possible suspension of cross-border operations.	Customers fear loss of protection when their data leaves their legal jurisdiction.
Algorithmic Bias	Fear that AI-driven personalization may reinforce inequalities or discriminate.	Regulatory scrutiny, reputational damage, potential lawsuits for biased decision-making.	Perception of unfair treatment reduces willingness to engage with AI-driven services.

GDPR and CCPA: Frameworks for Consumer Trust

The increasing concern over data privacy within the digital economy has prompted governments to foster regulatory frameworks that are designed to protect people by holding financial institutions accountable for how they use the personal data that they collect. GDPR in the European Union and CCPA in the United States are the two most influential within the banking sector. The laws share a common obligation, which is to restore control of personal information to consumers (Wong *et al*., 2023) [7]. However, there is a variation in scope, application, and unique rights that have been integrated. Lastly, they contain a unique application of the effects they have on Artificial Intelligence banking marketing.

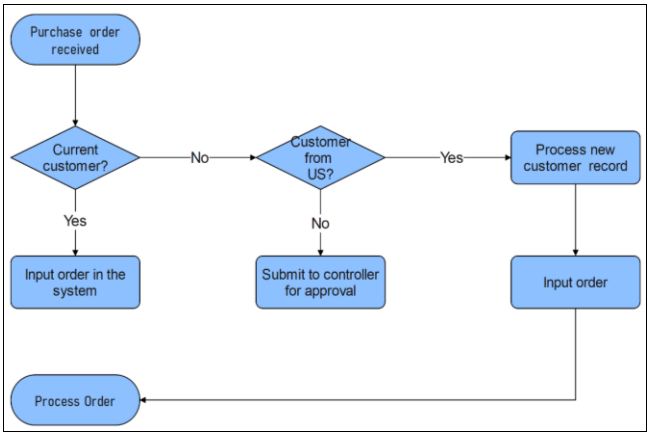

Fig 3: AI-Driven Personalization Process in Banking

GDPR (European Union)

GDPR was established in 2018 as the most comprehensive data protection regulation globally. The framework provides individual with a wide range of rights over their personal data. They include accessing their own data, making necessary corrections, deleting information (right to be forgotten), and restricting how the information they provide will be used (Abdulsalam & Tajudeen, 2024) [1]. In GDPR is central where organizations are required to acquire explicit permissions prior to processing any personal data. The regulation is applicable not only to organizations that are part of the European Union. However, the jurisdiction is also applicable to firms that take part in processing data pertaining to European citizens since it has a global reach (Yusuff, 2024) [8]. For financial institutions such as banks, GDPR calls for the reconfiguration of data collection practices and the use of different practices. Ultimately, it becomes easy to ensure the personalization approach employed is transparent, explainable, and aligned with the consent of the consumers.

CCPA (California)

CCPA was enacted in 2020, and it depicts similar values that might not be applicable to the United States Context. Attention is directed towards consumer rights in the state of California. Residents of the state are granted the rights to know the type of data that is being collected about them, request any deletion to be made, and opt out of the sale or sharing of information (Abdulsalam & Tajudeen, 2024) [1]. CCPA is less strict compared to GDPR, but requires business entities, including banks, to offer clear notices on how they intend to use the information they gather while providing their customers with choices that are actionable regarding the sale or transfer of their data (Srivastava & Sharma, 2024) [6]. While CCPA is currently applicable to California residents, the effects it has in increasing by inspiring most states in the U.S. to draft similar laws. Attention is being directed towards signaling the wider movement towards a more solid consumer privacy

protection action.

Impact on Banking Marketing

For banking marketing that is AI-driven, the regulations are important in defining a balance between personalization and privacy. There is an imposition of restrictions towards hyper-personalization through requiring explicit consent, transparency, and minimization of data. Banks can no longer assess customer data indiscriminately for their own marketing gains without depicting any form of compliance (Abdulsalam & Tajudeen, 2024) [1]. Alternatively, the framework creates an opportunity for building customer trust, which should be integrated into ethical operations that are personal to the strategy being used. Offers are generated through transparency, which provides clarity on how the data will be used, and respect for the choices made by the customer will be established (Zungu *et al*., 2025) [9]. The end goals are to have a competitive advantage in the market. If the Artificial Intelligence personalization is aligned with GDPR and CCPA principles, financial institutions can differentiate themselves as custodians that are more responsible for customer information. In the end, it becomes possible to solidify loyalty in an era of heightened privacy awareness.

The table below makes a comparison between GDPR and CCPA. It highlights some of the essential provisions and their unique implications for Artificial Intelligence banking marketing.

Table 2: Comparison of GDPR and CCPA in the Context of Banking Marketing

Aspect	GDPR (EU)	CCPA (California)	Implications for Banking Marketing
Scope	Applies to all companies processing data of EU citizens, regardless of location.	Applies to for-profit businesses meeting certain revenue/data thresholds in California.	Global reach of GDPR forces multinational banks to adopt universal standards; CCPA creates U.S. baseline.
Consumer Rights	Access, correction, deletion ("right to be forgotten"), data portability, restriction of processing.	Right to know what data is collected, opt out of sale/sharing, request deletion.	Both require banks to provide mechanisms for data access and deletion; GDPR grants broader rights overall.
Consent	Explicit consent required before processing personal data.	Implicit collection allowed, but consumers can opt out of sale/sharing.	GDPR demands proactive opt-in for personalization, while CCPA allows default but requires opt-out choice.
Transparency Requirements	Detailed disclosures on data use, retention, and purpose required.	Privacy notices must disclose categories of data collected and uses.	Banks must communicate personalization practices clearly to consumers in both regions.
Penalties for Non-Compliance	Up to €20 million or 4% of global annual turnover, whichever is higher.	Up to $7,500 per intentional violation; $2,500 for unintentional violations.	GDPR penalties create higher financial risk; both frameworks impose reputational damage.
Cross-Border Data Rules	Restrictions on transferring data outside the EU unless protections are ensured.	No equivalent cross-border restrictions.	Banks operating globally face stricter operational constraints under GDPR.
Impact on AI Personalization	Requires explainability of algorithmic decisions; "black box" AI discouraged.	Less explicit but encourages clarity in data use.	Banks must prioritize explainable AI to align with GDPR; CCPA places less emphasis but still pressures transparency.

Balancing Act: Personalization with Privacy

The most challenging issue that banks face when adopting AI-driven marketing is not if to consider personalization, but how to do so in a manner that is respectful. Consumers are constantly in need of meaningful and customized experiences, but equally demand privacy, transparency, security, and ethical use of their data. Creating a balance requires banks to go over and beyond complying with the provided regulations and embedding trust-built practices into the design of their personalized strategies (Srivastava & Sharma, 2024) [6]. The four main pillars needed to create a privacy-first approach to personalization include transparency, consent, data minimization, and explainability.

Transparency

A cornerstone of consumer trust is transparency. Customers need to constantly understand that the data being collected, processed, and applied is suitable for creating personalized offers. When banks take shelter behind Artificial Intelligence models that are opaque and vague in nature, they end up building suspicion. In comparison, financial institutions that have capitalized on providing accessible and easy-to-read explanations of their strategy being used in personalization end up building trust with the customers (Abdulsalam & Tajudeen, 2024) [1]. Transparency equally builds on real-time disclosures, where they explain why a particular commodity is being recommended.

Consent and Control

Instead of assuming that customers are comfortable with the data-driven marketing approach, banks need to offer a more meaningful control over the information that they gather in the process. There should be consent management frameworks that allow users to opt in to personalization. The approach will depict respect for autonomy (Wong *et al*., 2023) [7]. Nevertheless, customer need to have ongoing control since it will grant them the ability to make changes to their preferences or exit when they need to do so. The active participation not only fulfills the legal needs. Instead, it equally builds on customer relationships, as customers will end up feeling empowered as opposed to being surveyed.

Explainable AI

Explainability is one of the crucial elements that are part of Artificial Intelligence personalization. The domain uses a black-box algorithm, which makes recommendations in the absence of justification and ends up being perceived as manipulative and unfair. Banks can mitigate the effects by adopting explainable AI (XAI) approaches that offer customers an understandable reason as to why they are being prompted with the offer (Srivastava & Sharma, 2024) [6]. For instance, a message that states, "We're offering you this savings product because your recent account activity shows consistent monthly deposits," will allow customers to foster a connection with the recommendation.

Table 3: Best Practices for Balancing Personalization with Privacy in Banking Marketing

Principle	Practical Application	Consumer Benefit	Banking Outcome
Transparency	Provide clear explanations of how data is used in personalization (e.g., "why am I seeing this?" pop-ups).	Builds confidence that data use is ethical and purposeful.	Strengthens reputation as a trusted financial partner.
Consent & Control	Implement opt-in personalization, preference dashboards, and easy withdrawal options.	Empowers customers to control their data and marketing experiences.	Reduces regulatory risk and builds long-term loyalty.
Data Minimization	Limit collection to essential data points (e.g., transaction history instead of location tracking).	Reduces anxiety about over-collection and misuse.	Lowers data storage/security costs and reduces exposure in case of breaches.
Explainable AI	Use explainable algorithms and provide simple justifications for personalized offers.	Increases understanding and trust in recommendations.	Improves engagement rates and compliance with emerging AI transparency requirements.
Regular Audits	Conduct internal reviews of data use, personalization algorithms, and compliance with privacy laws.	Reassures customers that safeguards are ongoing and not one-time.	Demonstrates accountability, satisfying regulators and investors alike.
Ethical Boundaries	Avoid personalization based on sensitive data (e.g., health, divorce, or political activity).	Prevents "creepy banking" effects that erode trust.	Reduces reputational backlash and ensures marketing remains supportive, not invasive.
Customer Education	Offer guides or tutorials explaining personalization benefits and data protections.	Increases comfort with opting into personalization.	Enhances adoption rates of AI-driven services by reducing fear of misuse.

Conclusion

The increase in Artificial Intelligence in banking marketing demonstrates both the extraordinary capability of technology and the fragility of consumer trust is not used accordingly. If financial behaviours are assessed, spending habits are evaluated, and life events are incorporated, banks can deliver and deeply personalized offer that will be viable in enhancing customer experience that equally strengthens loyalty. The same personalization might also become a liability when the loyalty of the consumer is perceived to be intrusive, manipulative, and unsafe.

In the context of regulatory frameworks such as the General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA) should not be perceived as a hurdle in compliance. Instead, they need to act as a roadmap for responsible data practices that can contribute towards granting a financial institution the needed competitive advantage. Embracing the two frameworks allows banks to showcase accountability while reinforcing their responsibility as custodians of financial data that is sensitive and cultivating trust in a period when customers and increasingly becoming sceptical about the use of digital technology.

Ultimately, the future of Artificial Intelligence marketing will define not only how much data a financial institution can gather but also highlight its responsibility when it uses it in different ways. Personalization that respects privacy will describe some of the most essential and successful banks by allowing them to stand out in a sector that is very competitive. In the financial sector, the currency of loyalty is customer trust. Embracing GDPR and CCPA, and other similar frameworks, offer guiding principles for financial institutions to use in transforming their regulatory obligations for the purpose of innovation and ensuring that the personalization and privacy correlate with each other.

References

1. Abdulsalam TA, Tajudeen RB. Artificial intelligence (AI) in the banking industry: A review of service areas and customer service journeys in developing economies. Business & Management Compass. 2024; 68(3):19-43.
2. Arrieta A. Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities, and challenges toward responsible AI. Information Fusion. 2020; 58(1):82-115.
3. Gyau EB, Appiah M, Gyamfi BA, Achie T, Naeem MA. Transforming banking: Examining the role of AI technology innovation in boosting banks' financial performance. International Review of Financial Analysis. 2024; 96(12):10-37.
4. Khan FS, Mazhar SS, Mazhar K, AlSaleh DA, Mazhar A. Model-agnostic explainable artificial intelligence methods in finance: A systematic review, recent developments, limitations, challenges, and future directions. Artificial Intelligence Review. 2025; 58(8):232.
5. Mu J, Liu D. Application of artificial intelligence technology in the field of digital currency security. Procedia Computer Science. 2024; 243(23):458-464.
6. Srivastava S, Sharma S. Customer trust and data privacy in digital banking services: A study in context of artificial intelligence. ShodhKosh: Journal of Visual and Performing Arts. 2024; 5(1):1515-1523.
7. Wong RY, Chong A, Aspegren RC. Privacy legislation as business risks: How GDPR and CCPA are represented in technology companies' investment risk disclosures. Proceedings of the ACM on Human-Computer Interaction. 2023; 7(CSCW1):article-82.
8. Yusuff M. Ensuring compliance with GDPR, CCPA, and other data protection regulations: Challenges and best practices. Journal of Data Privacy and Security. 2024; 18(4):112-130.
9. Zungu NP, Amegbe H, Hanu C, Asamoah ES. AI-driven self-service for enhanced customer experience outcomes in the banking sector. Cogent Business & Management. 2025; 12(1):24-50.