Article

Consumer Privacy, Ethics and Autonomy in a Digital Society

Evans O. Achara *

Posted Date: 16 June 2026

doi: 10.20944/preprints202606.1262.v1

Keywords: data mining; privacy; informed consent; algorithms; digital economy; internet of things IoTs; encryption; pseudonymization

 doi:10.20944/preprints202606.1262.v1

Article

Consumer Privacy, Ethics and Autonomy in a Digital Society

Evans O. Achara

Information Systems Technology, University of Phoenix, Phoenix, AZ, USA; oldscrow@email.phoenix.edu

Abstract

As enterprises continuously rely on data to effectively drive and power business processes in a digital economy, privacy concerns have emerged as a major source of deep concern among consumers and privacy advocates in a digital society. Several scholars have shared their opinions and perspectives in related articles on this issue since privacy is a fundamental and constitutional right in many countries that must be protected at all times. While several practitioners and industry experts have proffered various privacy-preserving measures to help empower users to make informed decisions that relate to the use of their personal information, others have proposed various privacy preserving measures and mechanisms to help protect the use of personal information in a digital society to create the necessary confidence and trust amongst members of the public. With the current advances in artificial intelligence, social media platforms, and automation, the issue has emerged as a major source of concern among policymakers, privacy advocates, and industry experts. The purpose of the e-Delphi study was to gain consensus from the opinions of industry experts on best practice measures and various effective privacy-preserving measures to help enhance users' privacy and allay privacy concerns in a digital society. The study adopted the Restricted Access/Limited Control (RALC) theory of privacy to provide a theoretical framework for the research study. The study included three rounds of questioning using the Delphi method. The findings from the study revealed that effective privacy-preserving measures, such as Data minimization, Privacy-By-Design, Privacy Labels and icons, Data Ownership and control, Third-party App Permission, Mandatory Data/Privacy Breach Notice, Frequent Policy Updates, End-to-End Encryption, User-Friendly Privacy Control features, and Informed Consent, provided an effective way to allay the fears of consumers in a digital age.

Keywords: data mining; privacy; informed consent; algorithms; digital economy; internet of things IoTs; encryption; pseudonymization

1. Introduction

The Digital Age is characterized by unprecedented levels of data generation, collection, and analysis. Advances in data mining, artificial intelligence, cloud computing, and ubiquitous connectivity have transformed data into a critical economic, strategic, and social asset. Organizations across sectors increasingly rely on data-driven insights to personalize services, optimize operations, predict consumer behavior, and gain a competitive advantage. While these developments have generated significant innovation and economic value, they have also intensified concerns regarding *consumer privacy and individual autonomy*. The need to protect privacy rights and data privacy in a digital age continues to be a subject of major concern [70,85].Data is referred to as the new oil in a digital economy. Organizations in various industries increasingly use all kinds of business intelligence software powered by sophisticated algorithms to help collect and analyze the volume of data generated daily. Application of data mining algorithms to several types of structured and unstructured data, from various sources, helps disclose hidden relevant information [14,73]. The convergence of data mining, consumer privacy, and autonomy represents one of the most critical challenges of the digital age. While data mining continues to drive innovation and economic growth, its unchecked application risks undermining fundamental rights and ethical norms. Understanding

 doi:10.20944/preprints202606.1262.v1

how data mining practices affect consumer privacy and autonomy—and how policy, governance, and organizational strategies can mitigate these effects—is essential for developing sustainable, trustworthy digital ecosystems. The information discovered within the data is used to enhance decision-making abilities [14,43].

The current advances in digital space with artificial intelligence and machine learning allow for systematic processing, which includes clustering, logical or mathematical queries, summarizing, separation, distributions, correlations, and relationships, to gain deeper insight into the data [43,62–67]. Data mining is a knowledge discovery process to uncover hidden patterns, relationships, customer preferences, unknown correlations, and market trends to better serve users' needs. It offers businesses the opportunity to discover information from consumers, to better understand the dynamics of the business environment. The immense value and benefits of data mining analytics are realized when organizations use the information generated to enhance decision-making capabilities [5,78]. Data mining is not only the extraction of previously unknown information from a database but also the discovery of relationships that did not surface in previous methods of data analysis. Data mining processes are characterized into three distinct types: *Discovery, Predictive Modelling, and Forensic Analysis* [11,14].

With the current advances in digital technologies, with artificial intelligence and social media, the issue of privacy has become deeper amongst policymakers and privacy advocates. Primary sources of concern revolved around sharing personal or individual-specific data, such as names, locations, date of birth, age, address, demographics, lifestyle, and interests, without consumer consent. Consumer privacy occurs and exists when individuals can limit access and control the release of information about them [47,62]. An invasion of privacy occurs when control is lost or unwillingly reduced due to a marketing transaction [68]. The two key assumptions underlying privacy are (i) Most consumers would like to have more control, and (ii) Giving consumers more control over how information about them is used will alleviate their privacy concerns. The issue of privacy in the digital age is an important subject that has generated concerns amongst privacy advocates [11,12,68]

In a landmark settlement deal, brought by privacy advocates attorneys against Alphabet Inc., the parent company of Google. Google Inc. reached a $391.5 million settlement deal with 40 US states due to its monetization of "location history data" of consumers, providing advertisers and other third-party organizations with consumer location history, users who viewed and visited advertised stores [17,84,85]. Privacy advocates argued that location history tracking is one of the most sensitive personal pieces of information of consumers and constitutes a major privacy breach, such cases have continued to evolve and pit privacy advocates against various digital companies both in the US and the EU (European Union). As the current advances in digital technologies with artificial intelligence continued to enhance the ability of organizations to easily collect and share consumer data to better provide quality services, the need to allay the fears of consumers and privacy advocates on its impact on privacy lies on how organizations can put transparency at the fore-front of their business process practice [85,88]. The need to get a deeper insight and gain commercial value from the large volumes of data generated to help improve business process performance often allows enterprises to collect consumer data indiscriminately [14,31]. Also, the lack of clear consumer consent and adequate implementation of data-sharing policies created a loophole for enterprises to share users' data with third-party organizations, without appropriate consent. It becomes increasingly clear that as advances in digital technologies continue to shape the society with the current advances in artificial intelligence, machine learning, and automation, privacy concerns will continue to take the center stage amongst industry watchdogs, privacy advocates and policy maker as the application of information and communication technologies (ICT) in social and businesses platforms increases in future [8,52,53].

 doi:10.20944/preprints202606.1262.v1

2. Literature Review

The pace of the proliferation of digital content and its negative impacts on privacy has been a subject of major concern amongst scholars, policymakers, and industry watchdogs [3–14,21]. At the core of these privacy concerns is data mining—the systematic extraction of patterns, correlations, and predictions from large datasets—which often involves personal and behavioral data generated through everyday digital interactions [41]. The continuous advances and proliferation in the digital ecosystem, leading to the expansion of data mining practices, have reshaped the relationship between individuals, organizations, and digital systems, raising fundamental questions about *control, consent, transparency, and power* in the digital ecosystem. The right to privacy is a fundamental human right that should be protected in the current digital age [63,82]. Data is seen as the new gold, and data privacy is a major source of concern to all stakeholders. Privacy advocates argue that a privacy framework requires the processes used in gathering and disseminating information to be two-fold: (a) *Appropriate to a particular context* and (b) *Comply with norms that govern the flow of personal information in each* context [33]. In the digital economy, data mining techniques are embedded in Online platforms and social media, E-commerce and digital marketing systems, Financial services and credit scoring, healthcare analytics and personalized medicine, Smart devices, IoT systems, and mobile applications. These various systems continuously collect both *explicit data* (such as user-provided information) and *implicit data* (such as behavioral traces, location data, and interaction logs). And through machine learning and predictive analytics, data mining transforms raw data into actionable insights, often enabling automated decision-making at scale [11,39].

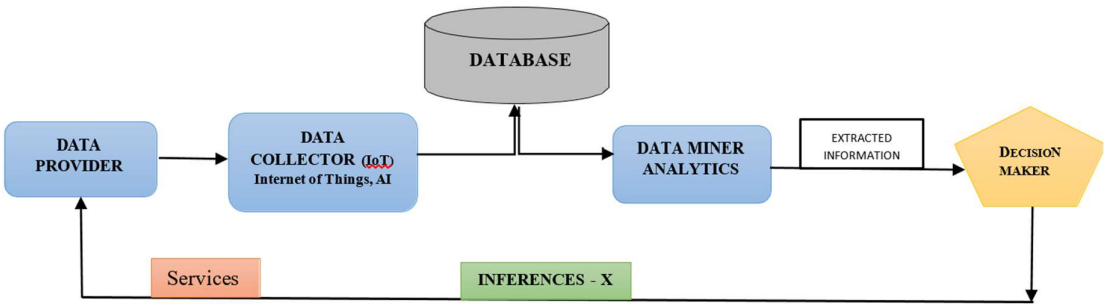

Figure 1. Data mining analytic processes.

2.1. Historical Content

Historically, information is power, and both collecting, storing, and collating personal information are means of acquiring power [16,28]. In the early 1960s to 1980s, this was the era of mainframe computers, and early databases marked the first major shift in data practices. Governments and large organizations began digitizing records related to taxation, health, employment, and social services [31]. While data mining as a discipline had not yet emerged, concerns grew amongst privacy advocates about centralized data repositories and the potential for misuse. Data mining in its early stage was seen as a great technology with the opportunities it offers, and the greatest challenge facing it was making the transition from being an early market technology into the mainstream. Historically, the greatest early opportunity facing technology was the vast collection of data from websites such as Yahoo, collecting over [88,95]. Consumers always believed and anticipated that privacy loss would be a greater problem in a digital age, and privacy concerns sometimes might influence users to provide spurious information even though data mining services require accurate input for results to be meaningful [62,82–95].

2.1.1. Privacy Concerns in the Digital Age

With the rapid advances in the digital technology with social media, artificial intelligence (AI), big data, and automation, a breach of privacy might occur when individuals are not aware that their

 doi:10.20944/preprints202606.1262.v1

data have been collected and passed on to other organizations and used for purposes other than the one for which they were initially collected [2,63]. As data mining increasingly become an indispensable component of the digital economy, and its expansion has fundamentally altered the balance between innovation, privacy, and individual autonomy, Privacy advocates have increasingly voiced their concerns at various opportunities about the impact of data mining on privacy in a digital age. The digital age demands a reexamination of how data is governed, how consent is operationalized, and how autonomy is preserved in increasingly automated and data-driven environments [32,46]. Data mining challenges this control by: Aggregating data across multiple sources, Inferring sensitive attributes from non-sensitive data, and Repurposing data beyond its original context. Privacy concerns have increasingly revolved around *informational self-determination*, which is the ability of individuals to control how their personal data is collected, used, shared, and retained. Datamining challenges this control by: Aggregating data across multiple sources, Inferring sensitive attributes from non-sensitive data, and Repurposing data beyond its original context. Addressing these concerns requires interdisciplinary inquiry, combining insights from technology, law, ethics, behavioral science, and organizational governance [68,71].

2.1.2. Privacy-Value Trade-Off

A significant part of the privacy concerns often voiced amongst privacy advocates is the privacy value trade-off. The rapid proliferation and deployment of various digital technologies that continuously undermine privacy by business enterprises threaten to make informational privacy obsolete [68,95]. The need for a more robust, meaningful definition of privacy becomes more important to satisfy genuine concerns, as electronic data about individuals becomes increasingly detailed and as technology enables more powerful collection and curation of these data [94,95]. There is a privacy-Value trade off as digital services are often offered in exchange for personal data, creating a perceived trade-off between convenience and privacy. Consumers may consent to extensive data collection to access services, discounts, or personalization, even when they do not fully understand the scope of data mining practices. In the digital economy, personal data functions as a form of currency, enabling organizations to deliver tailored products, targeted advertising, predictive services, and data-driven innovation [87,88]. This exchange has become a foundational business model for many digital platforms and data-intensive industries. This dynamic raises concerns about whether consent is genuinely informed or merely procedural. While consumers often recognize the value derived from data driven services, the trade-off is rarely transparent or symmetrical. Individuals may consent to extensive data collection without fully understanding the scope, duration, or secondary uses of their data. Since the complexity of data mining practices is not always transparent to consumers, algorithmic inference and third-party data sharing limit consumers' ability to accurately assess long-term privacy risks. As a result, consent may be procedural rather than genuinely informed [65,96].From an ethical perspective, the privacy–value trade-off raises questions about fairness, autonomy, and proportionality. When access to essential digital services is contingent upon extensive data surrender, individuals may face coerced choices rather than voluntary exchange. This challenges the legitimacy of consent-based privacy models and calls for stronger structural protections. [56,60,61].

2.2. Importance of Data Protection and Privacy Laws

Data privacy-protection laws aim to protect consumers from being vulnerable through data in the hands of authorized or unauthorized businesses and to protect various members of society [65,68]. Consumer data protection and privacy laws seek not only to protect consumers but also to enhance the promotion of fairness, accountability, and transparency on the part of those handling, using, storing, and sharing consumer data [65,67]. Consumers may face possible risks from digital products and services that are non-transparent, such that informed consent alone may not adequately protect or guarantee adequate accountability, fairness, and transparency from digital service providers [50,97]. The argument is that without privacy, individual rights to freedom of expression and freedom

 doi:10.20944/preprints202606.1262.v1

of access to information are inherently threatened, and the possibility of living in a civilized, fair, and democratic society [14,68–82]. Privacy and data protection laws should guarantee adequate protection for consumers, regardless of whether there is informed consent from the consumer [8,47]. [50] Suggested three core fundamental principles of data protection and privacy laws: (a) *Purpose Specification,* (b) *Data minimization, and* (c) Treatment of data protected or special categories of people. (*Race, gender, religion, or groups*). Consumer protection and data privacy into three broad Phases: (i) *Pre-engagement phase*: This phase involve primarily what disclosures and information notifications need to be made known to consumers regarding the use of their data, what purpose, why the data is being collected, how it is being collected if it's going to be shared to third parties, and basic procedures for obtaining informed consents. (ii)*Engagement Phase*: This phase involves restrictions, carefully detailing responsibilities on the things organizations can do or not do with consumers' or users' data within their custody. (iii)*Post-engagement phase:* this phase discloses and details accountability measures for holding digital product and service providers, cloud computing organizations, and those using data analytics algorithms, machine learning, and artificial intelligence accountable for any violations of consumer protection and data privacy laws [47,50,51].

2.2.1. Data Privacy-Preserving Schemes

Preservation of privacy in data mining has emerged as an unconditional prerequisite for exchanging privileged information in data analytics [88]. The argument is that this privacy preservation scheme does not reveal the data owner's confidential information during the outsourcing process [95,98]. [75,97] Classified Privacy-preserving data mining techniques under the four major techniques of data anonymization, de-anonymization, perturbation, and cryptography.

2.2.2. Cryptographic Method

Employ secure-multi-party computation and uses Homomorphic Encryption (HE), Encryption-based technologies, Attribute-based encryption; Secure Two-Party Computing Protocol. Other privacy models: *K-anonymity,l-diversity,t-closeness,andedifferential privacy models* [2]. *Homomorphic encryption* technology was proposed as one of the most effective and direct means of protecting user privacy that can directly perform operations with results consistent with the results of operations [95,98].

Table 1. Illustrates a comparison of proposed privacy-preserving data mining techniques.

Techniques	**Method Employed**	**Data Mining Tasks**			
		Classification	**Clustering**	**Associated Rules**	**Regression**
Anonymization	Generalization, Suppression, Permutation				
Condensation	Aggregate, Rank				
SMC (Secure Multiparty Computation)	Homomorphic Encryption (HE), Circuit Evaluation & Sharing Scheme				
Pseudonymization	Cryptographic				
Perturbation	Adding Noise, Data Swapping, Global recording, Micro aggregation				
Randomization	Scrambling, Resampling				
Fuzzy Based	Clustering, Micro aggregation-regression				
Neural Network Based	Bayesian Network, Probabilistic Neural Network				

Privacy-preserving techniques help protect and preserve the integrity and sensitivity of the data's content. An important aspect of the privacy preserving technique is the confidentiality of the

 doi:10.20944/preprints202606.1262.v1

content of the data [2,66].Also other proposed privacy-preserving measures to enhance confidentiality include: *Encryption, Anonymization,* and Noise-based approaches [20,85].

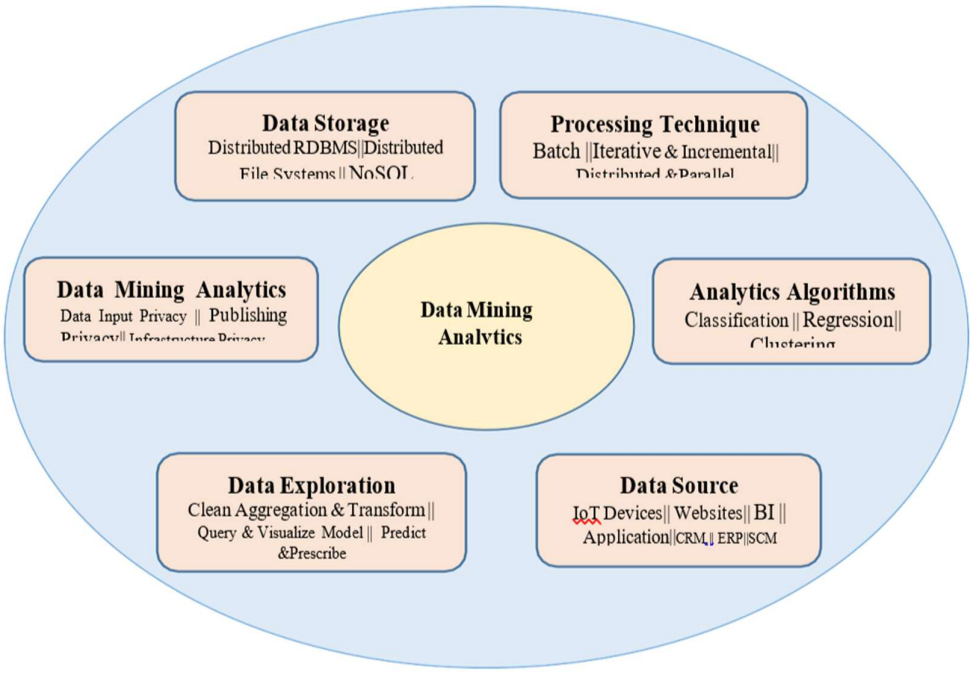

Figure 2. Taxonomy of data mining analytics.

2.3. Privacy Rights in a Digital Age

Privacy is a fundamental human right recognized in many international agreements and documents [68,82]. [29] Emphasized the impact of the international regulatory framework, such as the *GDPR, which* seeks to protect the privacy rights of individuals as a human right. The ACLU maintained that even though privacy laws at the international human rights level are extensively grounded and rooted in robust principles, they have not seemed to have been developed and adapted to adequately fit the needs of the current 21st-century digital society [1,22]. In line with the need to strengthen data privacy rights, the *European Union EU* strengthened its legislation with the enactment of the *General Data Protection Regulation* (GDPR) applicable in the law of member states [50].Other privacy advocates referenced the Fourth Amendment of the US Constitution for the protection of personal privacy [68]. The *right to be forgotten* (*RTBF*) is also seen as a privacy right concept, which at its core is fundamentally based on the rights to respect privacy, family life, and protection of personal data [23,65].

2.4. Protection of Consumer Autonomy in a Digital Economy

Autonomy and privacy often interact, and consumers always want to have certain control over their personal information. Privacy advocates have often maintained that there is a strong relationship between autonomy and privacy, as privacy and autonomy often overlap in context, and it is particularly important to note that when one's privacy is taken away, autonomy often goes with it [12,67]. Autonomy is closely tied to data practices, as personal data increasingly shapes the opportunities, choices, and outcomes individuals experience in the digital economy. Data mining can undermine autonomy when consumers lack meaningful choice or alternatives. Decisions are influenced by opaque algorithms. Behavioral profiling enables targeted persuasion or manipulation. When users entrust organizations with information, they make themselves vulnerable, and their vulnerability might increase the risk of information misuse, unauthorized disclosure, manipulation, or loss of autonomy[80].Lack of self-determination can invariably manifest when consumers feel they

 doi:10.20944/preprints202606.1262.v1

are unable to control their actions or take actions that make significant changes and impact the features of their environment [49,93–95]. Privacy advocates emphasized that if changes aren't made to protect and appeal to consumers' sense of autonomy and violation of privacy which data mining analytics and big datasets cause, the impending likely results might be future public outrage, which might subsequently elicit a regulatory crackdown from government parastatals on data mining and big dataset and the collection and use of consumer data, which poses a far greater threat to the innovative opportunities inherent in data mining and big data [12,30].

2.5. Consumer Data, and Privacy Rights in the Digital Age

In the Digital Age, data—particularly consumer data—has become a key economic and social resource. With the proliferation of digital platforms, online services, the Internet of Things (IoT), mobile applications, cloud computing, and artificial intelligence (AI), vast quantities of personal data are collected, processed, stored, and shared [65].This has created new opportunities for personalization, efficiency, and innovation, but also raised profound questions about privacy, autonomy, fairness, and control over personal information. Consumer data and privacy rights are therefore central to contemporary debates in technology governance, legal compliance, ethical business practice, and human rights protection [68,71].

Consumer data is the new gold in the digital age. Consumer data is referred to as any information that can be associated with an individual or group of individuals. And it includes the *Personal Identifiable Information (PII)*: Name, address, contact details, government IDs; *Behavioral Data*: Online activity, purchase history, browsing patterns; *Sensitive Data*: Health records, biometrics, financial data; *Location Data*: GPS, connectivity logs; *Derived Data*: Inferences about preferences, personality, or habits created through analytics. In a digital ecosystem that comprises manufacturing, production, communication, transaction, and any business process activities, data flows continuously, generating new insights and associated privacy risk [85,86].

2.5.1. Data Life Cycle in the Digital Era

Consumer data typically passes through phases: *Collection: Explicit (forms, registrations) or implicit (tracking, sensors),* ***Processing*****:** Analysis, profiling, algorithmic inference, ***Storage*****:** Cloud databases, distributed ledgers, third-party servers.

Sharing/Transfer: With partners, advertisers, and platforms. ***Deletion/Retention*****:** Policy-governed retention and deletion practices. At each stage, privacy and governance challenges arise, requiring legal and ethical oversight. With the current advances in digital technologies and increasing level of deployment of artificial intelligence with algorithms that also undermine consumers' sense of autonomy, privacy, and self-determination, consumers are increasingly becoming more vulnerable [4,85].

2.5.2. Privacy-Preserving Solutions

[2,98] cite possible ideal solutions for helping resolve data mining and big data privacy protection issues into three different categories: (a) *Federated learning,* (b)*Encryption-based technologies*, and (c) *Differential privacy technologies*. Privacy violations are not caused by the revelation of big personal secrets but by the disclosure of many cumulative small facts in a row and the lack of trustworthy privacy safeguards in many current services [37,82].

2.6. Privacy Rights: Legal and Ethical Foundations

Privacy rights have been referred to as a fundamental human right. Privacy rights are recognized in various legal instruments and jurisdictions: *Universal Declaration of Human Rights*: Right to privacy, *Regional Laws*: GDPR (EU), CCPA/CPRA (California), PDPA (Singapore), LGPD (Brazil), PIPEDA (Canada),*Sectoral Laws*: HIPAA (health data), GLBA (financial data)[25]. These laws define consumer rights such as: *Right to access personal data, Right to correct inaccuracies, Right to deletion/erasure, Right to*

 doi:10.20944/preprints202606.1262.v1

restrict or object to processing, Right to data portability, Right to informed consent,Right to be informed about profiling/automated decisions.

Legal protection varies by geography and sector but increasingly emphasizes individual control and transparency [27]. *Technological and Ethical Design* - Privacy-by-design and autonomy-enhancing features should be part of product architecture as privacy preserving measures at the development stage, such as: Contextual consent flows, Explainable AI dashboards, Default privacy protective settings, User-accessible data logs and controls [15,18]. These measures satisfy legal expectations and promote ethical legitimacy. Other Legal Responses- Government put in place in view of the escalating concerns, governments introduced stronger data protection laws emphasizing individual rights, transparency, and accountability. These frameworks recognized that data mining posed systemic risks to privacy and autonomy that individual consent alone could not mitigate. *Ethical Reframing* - Ethical discourse expanded to address: Power asymmetries between data collectors and individuals, Fairness and bias in data-driven decisions collective and societal impacts of surveillance. Privacy became viewed as a collective good, essential to democratic governance and social trust [59,65].

2.7. Big Data and Data Mining Analytics in Business

In the current digital economy, all businesses thrive on data-driven decisions with data mining serving as a source to uncover hidden business process information and gain knowledge for making informed decisions [3,87–91]. The immense value data mining provides to enterprises in various industries can never be overemphasized, from Healthcare, Manufacturing, Business Analytics, Retail, Oil and Gas, Telecommunications, Legal, and Financial Services. As a knowledge discovery process, data mining helps enterprises to remain competitive in various industries. Other benefits include detecting fraud, risk assessment, product retailing, supply chain management, and discovering previously unknown valid patterns and relationships [65,96].Businesses in various industries employ a range of data mining techniques, such as: *Classification*: Assigning data into predefined categories (e.g., credit risk assessment), *Clustering*: Grouping similar data points (e.g., customer segmentation), *Association Rule Mining*: Identifying relationships between variables (e.g., market basket analysis)[32,52]

Regression Analysis- Predicting numerical outcomes (e.g., demand forecasting), *Anomaly Detection*: Identifying outliers (e.g., fraud detection*),Text and Sentiment Analysis*- Extracting meaning from unstructured data[31]. These techniques are increasingly powered by machine learning and AI, enabling continuous learning and adaptation. Business applications of big data and data mining analytics include: Strategic Decision-Making- Big data analytics supports evidence-based strategy by enabling, Market trend analysis, Competitive intelligence, Scenario modeling and forecasting, Executives increasingly rely on analytics-driven insights rather than intuition alone. *Customer Analytics and Personalization - Businesses leverage data mining* to: Understand customer behavior and preferences, Deliver personalized recommendations and marketing, Improve customer retention and lifetime value. This has become central to digital platforms, e-commerce, and service industries. *Operational Efficiency and Process Optimization - Analytics enables*: Predictive maintenance in manufacturing, Supply chain optimization, Inventory management, Process automation and performance monitoring[34,56]. These applications reduce costs and improve responsiveness and agility.

Risk Management and Fraud Detection - Data mining identifies patterns indicative of: Financial fraud, Cybersecurity threats, Credit default risk, and Compliance violations. Early detection reduces financial and reputational losses. *Innovation and New Business Models*- Big Data enables: Data-driven product and service innovation, Platform-based and subscription business models, Monetization of data assets.[31,42–44]

In many cases, data itself becomes the core value proposition. *Organizational Capabilities and Infrastructure - Technological Infrastructure*, Effective Big Data analytics requires: Cloud computing and distributed storage, Scalable data processing frameworks, advanced analytics and AI platforms. Integration across legacy and modern systems remains a key challenge. *Skills and Human Capital* -

 doi:10.20944/preprints202606.1262.v1

Organizations must develop: Data science and analytics expertise, Domain knowledge to contextualize insights, Cross-functional collaboration between IT, business, and leadership. The shortage of skilled professionals remains a barrier to adoption. *Data Governance and Management*- Strong governance is essential to ensure: Data quality and consistency, Security and access control, Compliance with privacy and regulatory requirements. Without governance, analytics initiatives risk producing misleading or harmful outcomes. *Strategic Challenges and Limitations* - Despite its potential, Big Data analytics presents challenges: High implementation and maintenance costs, Data silos and integration complexity [15,23–25].

Overreliance on quantitative insights without contextual understanding, Risk of *"analysis paralysis"* or misleading correlations. Successful organizations align analytics initiatives with clear strategic objectives and organizational readiness. The future of Big Data and data mining analytics in business includes: Greater integration of AI and automation, Real-time, edge-based analytics, Explainable and responsible AI systems, increased regulatory oversight and ethical governance, Analytics will increasingly shift from supporting decisions to co-creating and automating decisions, heightening the importance of trust and accountability. By transforming vast diverse datasets into actionable insights, organizations can improve performance, innovate, and compete effectively in dynamic markets. However, the full potential of analytics can only be realized when technological capability is matched with organizational maturity, ethical responsibility, and robust governance. In a digital age, sustainable business value from data depends not only on analytical power, but on how responsibly and transparently that power is exercised [2,95].

2.8. Ethical Concerns with Algorithms in Business Process

Ethical issues and concerns of data mining with consumer privacy in the digital age require moral or ethical analysis in which the dilemmas contained in these issues are clarified and fundamental solutions are proposed for them [53,54]. Ethics is the moral principle that governs the behavior and actions of an individual or business enterprise. Computer ethics analyzes the moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use [44]. Ethics is the study of what ought to be done, using three distinct categories from different scholars, *first*, as a guided action of a fixed set of duties, rules, and policies. *Secon*d, from a teleological perspective, an "action that will bring the most good to the majority or a people that is deemed the most important" is described as a Utilitarian approach. *Third*, using the virtue model of ethics tends to influence people in the absence of clear rules, regulations, and guidance, and is motivated by instinct or spiritual will to do the right thing [54].

2.8.1. Ethical Foundations

Beyond legal compliance, ethical frameworks highlight: *Autonomy and dignity*- Respecting individuals' control over their information, *Fairness*- Avoiding discrimination through algorithmic profiling, *Transparency*-Clear, understandable data practices, *Accountability*- Organizational responsibility for data misuse. Ethics extends protections beyond what the law may explicitly require [40,41]. *Data Proliferation and Surveillance* - The scale and velocity of data collection have grown exponentially, often without consumer awareness or meaningful control. Surveillance capitalism describes a system in which data is extracted and monetized, often prioritizing corporate interests over personal privacy.

2.8.2. Algorithmic Decision-Making and Profiling

AI and machine learning transform data into profiles and predictions used in credit scoring, employment screening, targeted advertising, and risk assessment [15]. These raise questions about: *Transparency and explain ability, Fairness and bias, Unintended consequences and discrimination*, *Data Sharing and Third-Party Risks* - Data often flows through ecosystems of platforms, analytics services, advertisers, and partners. Consumers rarely understand the extent of these transfers, raising issues

 doi:10.20944/preprints202606.1262.v1

of consent validity and liability in case of misuse or breaches [44]. Parts of the concerns for privacy advocates involve: *Cross Border Data Flows and Jurisdiction* — The internet is global, but data laws are local. Divergent legal regimes (e.g., GDPR vs. U.S. sectoral approach) create complexity for multinational compliance and raise questions about: Where data is "located" legally, which jurisdiction applies, how cross-border protections are enforced, Security Risks, and Data Breaches[24,27]. High-profile breaches demonstrate the vulnerability of personal data, leading to financial loss, identity theft, reputational damage, and erosion of trust. *Security Risks and Data Breaches*-High-profile breaches demonstrate the vulnerability of personal data, leading to financial loss, identity theft, reputational damage, and erosion of trust.

2.9. Laws, Policies, and Regulations, as Privacy- Preserving Measures

Data governance policies are necessary privacy measures to avert unwanted sharing of data collected through the public domain, and should not be readily swapped between private and public partners due to privacy and confidentiality requirements. [23,63]. Other privacy laws *General Data Protection Laws* inspired by the GDPR, Argentina's *Protection of Personal Information Act* (POPIA), Japan's *Protection of Personal Information Act* (APPI), South Korea's PIPA Act, and the Australian *Privacy Principles* (APPs) privacy protection policy that stipulates for mandatory notification procedure for data breaches, considering the sensitivity of the information [29,36]. Privacy laws like the *California Consumer Privacy Act*,provides that upon request from a consumer an organization must disclose the categories and specific pieces of personal information the business has collected about a consumer, from the source the business or commercial purpose for collecting and any third party with whom the business shares such information [26,63]. Some of the applicable data protection Federal laws: *The Federal Trade Commission Act (FTC) of 1994* (FTC, 2006), *Electronic Communication Privacy Act (ECPA) of 1986 [19], Computer Fraud & Abuse Act (CFAA) of 1986 [19], Children's Online Privacy Protection Act (COPPA) of 1998 [19], Control Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAN) 2003 [19]. Fair and Accurate Credit Transactions Act (FACTA) of 2003.* These policies and laws help to serve as guardrails to enhance consumer privacy against the indiscriminate use of data that might, in turn, lead to a breach of privacy[18].

General Data Protection Regulation (GDPR) – A Global Benchmark. The EU's GDPR is widely considered the world's most comprehensive privacy law: Broad territorial scope, High standards for consent, significant enforcement penalties, and established data subject rights. GDPR has influenced other jurisdictions' laws and privacy-by-design requirements. *California Consumer Privacy Act (CCPA/CPRA).* Enhances privacy rights in the U.S. at a state level, emphasizing: Consumer choice in data use, Opt-out rights for data sales, Transparency, and disclosure. *Standards and Best Practices*-Industry standards and best practices serve as a regulatory framework providing guidance and oversight over practices within various industries. These standards and best practices in various industries guide most enterprises' business process practices, serving as industry compliance and privacy frameworks [59]. Organizations also adopt these compliance privacy frameworks to ethically guide data storage, use, and transfer during business by-Design (engineering principle), and NIST Privacy Framework [31,42]. These complement legal frameworks and operationalize compliance. Such as *Consent Management and Transparency,* Organizations must design systems that obtain *valid consent*, present clear privacy notices, and allow meaningful opt-out mechanisms. *Data Minimization and Purpose Limitation:* Collect only what is necessary and use data only for clearly defined purposes. *Governance, Accountability, and Risk Management*; Senior leadership, data protection officers, and cross-functional privacy councils are essential to enforce governance and audit compliance. *Privacy Engineering and Security Controls;* Technical controls such as encryption, anonymization, access controls, logging, and monitoring are core to protecting consumer-data.[38,60].

2.9.1. Consumer Rights in Practice

Exercising Data Subject Rights. For consumers to exercise data subjects over their information held in various enterprise databases. Consumers may seek access to their data held by organizations,

 doi:10.20944/preprints202606.1262.v1

Correction or deletion of data, and transparency reports about usage and sharing. Implementation challenges include identity verification, complex data architectures, and automation[25,60]. A significant part of consumer rights in the US is protected by various laws, rules, and regulations, enforced by various government agencies such as the *Federal Trade Commission (FTC),* including the *Fair Credit Reporting Act(FCRA), which* enforces and promotes, upon request, accurate and private information in files or databases of various credit reporting organizations. Also, the *Fair Debt Collection Practices Act* (*FDCPA*) - which is a defining Law on information on debt collection in the US applies strict adherence to consumer privacy on personal, family, and household debts. While the *Fair Credit Billing Act (FCBA)* and *Electronic Fund Transfer Act (EFTA)* establish procedural acts that guide the resolution of mistakes on credit billing and electronic fund transfer account statements, the *Equal Credit Opportunity Act (ECOA)* strictly prohibits credit discrimination based on sex, race, national origin, age, marital status, and religion [19]. There is a fundamental *Structural Power Imbalance,* as the asymmetry of power between data collectors and data subjects in a digital economy. *Large platforms and organizations* possess superior technical expertise, Extensive data aggregation capabilities, and control over digital infrastructures. Consumers, by contrast, often have a limited understanding of data mining processes and a limited ability to contest or opt out of them. This imbalance challenges traditional notions of free choice and informed consent[18,46].

2.9.2. Ethical and Behavioral Dimensions

Many consumers are unaware of privacy risks or the implications of consent. Behavioral economics shows that privacy fatigue and dark patterns often undermine consent legitimacy. The ethical and behavioral dimensions of privacy examine why privacy matters, how individuals perceive and respond to data practices, and whether digital systems respect human autonomy, dignity, and fairness [40,56–61]. Since privacy is widely understood as an extension of human dignity and personal autonomy, ethically, it enables individuals to: Control personal boundaries, Exercise freedom of thought and expression, and avoid undue surveillance or manipulation.[2] *Key ethical principles* in digital privacy arise within industrial practice, and several ethical principles guide responsible data practices: *Autonomy*: Individuals should have meaningful control over how their data is collected and used, *Informed Consent*: Consent must be voluntary, understandable, and revocable, *Beneficence and Non-maleficence*: Data practices should benefit users and avoid harm, *Justice and Fairness*: Data use should not reinforce discrimination or exclusion, *Accountability*: Organizations must be answerable for privacy impacts and failures. Ethical tension arises when commercial incentives, technological capability, and user welfare conflict. Behavioral Dimensions of Privacy revolves around the actions of individuals and their actions towards ensuring privacy [25,46–56]. A central behavioral phenomenon in digital privacy is the *privacy paradox*: this contends that individuals often express strong privacy concerns yet engage in behaviors that expose personal data, such as sharing information on social media or accepting broad terms of service [86].

2.9.3. Theoretical Framework

The privacy theories that provide the lens for this research study can be summarized in the following perspectives: (i) *Normative (zones and spaces)* (a) Lack of Intrusion (b) Right to Seclusion – Non-interference. (ii) *Descriptive (Repositories of data)* (a) Control of one's data(b) Limited access to one's data. (iii) *Situational/Contextual* (a) Privacy within a situation/context (storage/access –entering data on the website) (b) New Technology introduced-personal data unexpectedly made available or revealed [45,83].

2.9.4. Privacy Theories and Philosophical Conceptions of Privacy

Privacy is the right to be left alone, and privacy provides an umbrella under which to act freely. In the context of constitutional law, privacy is regarded as liberty or freedom to act in personal matters. Privacy may be observed from three different perspectives: (a) Privacy as undocumented

 doi:10.20944/preprints202606.1262.v1

personal knowledge, (b) Privacy as restricted access, (c) Privacy as control of information [55]. Privacy is not simply the absence of information about an individual; it is the control an individual has over information about himself or herself [35]. Privacy is claimed when individuals or groups determine for them information about them is shared and communicated to society [92]. [83] categorized privacy theories into four (4) distinct categories. (a) *The Non-Intrusion*, (b) *Seclusion,* (c) *Limitation,* (d) *Control Theories*. The benchmark of privacy is *contextual integrity:* which is that in any given situation, been transgressed or violated (a) *Norms of appropriateness*, and (b) *Norms of flow or distribution,* maintaining that contextual integrity is maintained that when both types of norms are upheld in any giving situation[46,61]. The plausibility of a right to control information about oneself, even one that is limited and constrained by other competing or countervailing rights and obligations, rests on the premise "individual autonomy, dignity, and personal liberty require that persons have the capacity to determine for themselves when, how, and to what extent information about them is communicated to others" [57,58].

3. Research Methodology, Population and Sample

The study used a qualitative e-Delphi research approach to derive a consensus from an expert panel and professionals on best practices to enhance privacy and automation, and privacy preserving techniques to help enhance consumer privacy and autonomy in a digital age. For this research study, a group of 26 industry experts from diverse professional backgrounds within the information technology (IT) industry was asked to share their perspectives on the subject of the study.

Determine Level of Consensus

To determine the level of consensus of the experts' opinion, the mean score of the opinions on each category and subcategory was determined. *Kendall's (W) Coefficient of Concordance* was used to determine the level of consensus. *W* ranges from between 0 to 1:

$$S = \sum_{i=1}^{n}(Ri - R)^2 \quad (1)$$

Ri = Total ranks of factors; m = number of rank sets (5-point Likert-type scale); and n = number of ranked factors. *Kendall's Coefficient of Concordance (W)*:

For *Strong Consensus*: *W*>0.7,

For *Moderate Consensus: W*=0.5; *and*

For *Weak Consensus*: *W*<0.3

$$W = \frac{12}{m^2(n^3-n)} \quad (2)$$

4. Data Collection and Analysis

Round one provide participants an opportunity to share their thought and perspectives on the subject of the study with open-ended questions. Nvivo was used to organize, analyze, and categorize privacy measures consistent with how participants responded about issues pertinent to the study. A 5-point Likert Scale is prepared for the second round, and a third for participants to affirm the effectiveness of the proposed privacy measures. The mean (m) and standard deviation (s) of participants' responses is determined for each of the proposed privacy-preserving measures.

 doi:10.20944/preprints202606.1262.v1

Table 2. Shows Mean of Proposed Privacy-Preserving Measures.

s/n	Privacy Preservation Measures	n	m	m²	S
1	Frequent Policy Updates & Disclosure	26	3.46	14.00	111.09
2	Right –To-Be-Forgotten Practice	26	3.42	13.58	103.20
3	Third-Party App Sharing Permission	26	3.81	15.81	143.85
4	Educational Awareness Campaign	26	3.07	11.77	75.67
5	Data Minimization	26	3.65	14.73	122.77
6	Anonymizers & Pseudonymizers	26	3.38	13.77	107.94
7	End-To-End Encryption	26	3.42	11.69	68.44
8	Language Simplification *Avoid Complex Legal Terms*	26	3.85	12.46	85.19
9	Privacy Labels & Icons:	26	3.42	14.31	115.99
10	Mandatory Data/Privacy Breach Notice	26	3.69	15.34	113.42
11	Transparency & Accountability	26	3.25	12.96	92.35
12	Auditing and Monitoring	26	3.12	12.34	83.72
13	User-Friendly Privacy Control Features	26	3.85	14.31	124.55
14	Data Ownership & Control	26	3.95	19.46	259.53
15	Privacy-By-Design(PBD)	26	3.61	16.65	163.07
16	Informed Consent pages	26	3.88	16.50	152.13
17	Strong Privacy Protection Laws &Enforcement	26	3.81	15.96	147.64
					Σ1886.1

The mean of the sum of all proposed privacy-preserving measures was determined m=3.56, and two (2) categories of proposed measures were identified. Those with a mean score below [3.5] and those with a mean score above [3.5]. Average mean (*m*) of [3.5] was adopted as a threshold to determine proposed measures for the third round survey. Proposed privacy preserving measures with a mean (m) score above 3.5 were grouped into a 5-point Likert-type scale for a round three survey to determine the consensus of experts on the effectiveness of these measures.

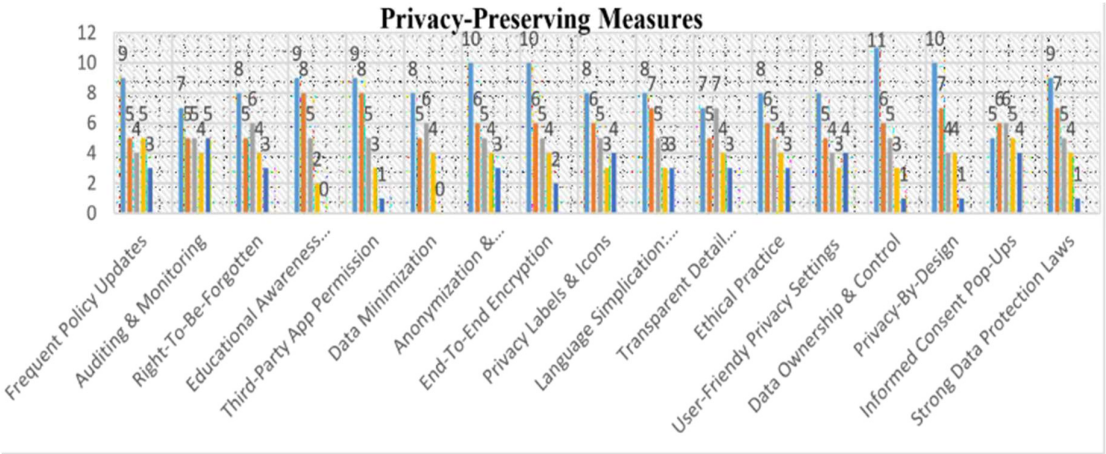

Figure 3. Responses on Privacy-Preserving Measures.

 doi:10.20944/preprints202606.1262.v1

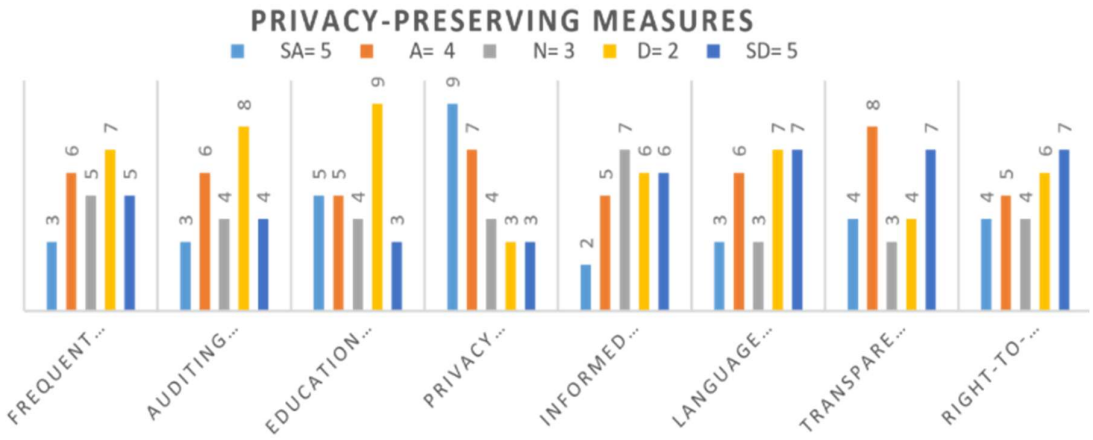

Figure 4. Privacy-Preserving measures with mean score below the threshold.

Proposed privacy measures with a mean score above the threshold of 3.5 have strong agreement amongst participants. These privacy measures were compiled and analyzed to determine experts' level of Consensus (*W*) on the impact of these measures when applied. Privacy-preserving measures with mean (*m*) scores above 3.5 were used to prepare a 5-point Likert-type scale. The study identified privacy measures that have a mean (*m*) score above the average mean of 3.5.Privacy measures with a mean score above 3.5 were used to prepare a 5point Likert-type scale for round three (3) survey. To determine the level of consensus among participant experts on the effectiveness of proposed privacy-preserving measures. Kendall's *(W).*The *Coefficient of concordance* (*W*) ranges from 0 to 1, (*W ≥0; and W*≤1).

$$W = 0.9;\ Approx. = 0.9$$

Kendall's Coefficient of Concordance (*W*), *W*=0.9; Where $W > 0.7$. This indicates a Strong Consensus amongst participants on the effectiveness of the proposed measures. Participants showed a strong level of consensus for the proposed privacy-preserving measure. The result ($W > 0.7$) indicated a strong consensus amongst participants on the impact of this proposed privacy preserving measure towards enhancing privacy in a digital society.

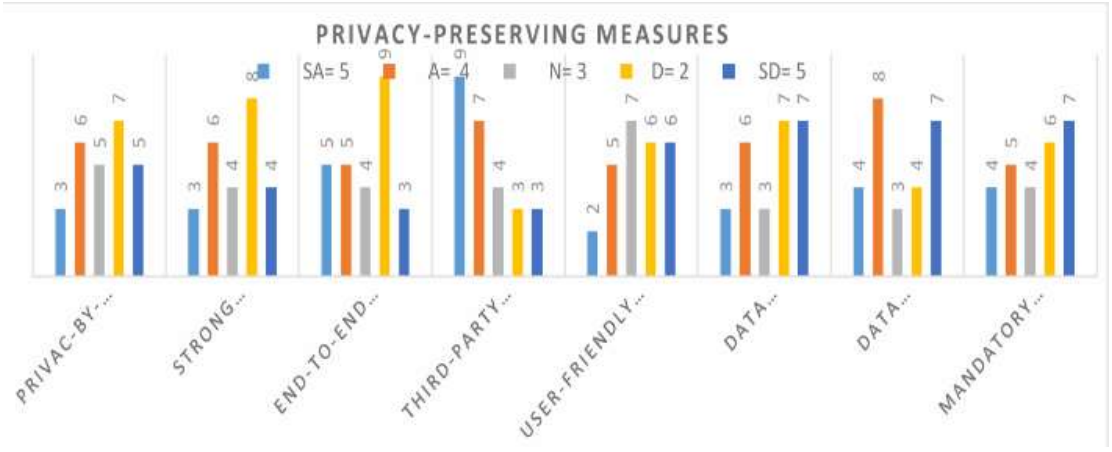

Figure 5. Privacy-Preserving Measures with Strong Consensus.

 doi:10.20944/preprints202606.1262.v1

Table 3. Privacy-Preserving measures with strong consensus.

s/n	Privacy-Preserving Measures	N	m	m²	S
1	Privacy By Design (*PbD*)	26	3.15	12.92	116.91
2	Strong Privacy Protection Laws &Enforcement	26	3.42	13.65	104.65
3	End-To-End Encryption	26	3.69	11.25	112.32
4	Third-Party App Sharing Permission	26	3.58	12.65	122.54
5	Informed Consent Notice *(Pop-Ups)*	26	3.88	13.25	112.10
6	User-Friendly Privacy Control	26	3.08	11.23	76.42
7	Data Minimizations	26	3.15	10.85	79.74
8	Data Ownership & Control	26	3.08	11.85	115.75
9	Mandatory Privacy Breach Notice	26	3.15	10.25	108.45
					Σ948.88

5. Limitations

A limitation of the study is that the views of the participants were subjective and highly dependent on individual experts' experiences. Another limitation is that the area of specialization and expertise of each participant shaped the view of the participants on the subject of the study and thus shaped their experiences. This limitation was addressed and mitigated through observation and collection of views common to all participants. The study provided deep insight into the subject of privacy in a digital society and the concerns shared by most professionals who participated in the study. Part of the limitations revealed while conducting the study included the respondents' ability to reply within the time frame of the survey process. The focus of the study was to determine consensus among the most common privacy measures proposed by the participants. A consensus of opinions of industry experts on the significance of privacy-preserving measures in a digital society. Include: *Privacy Protection Laws, Regulations & Implementation, Anonymization and Pseudonymization, User Education and Empowerment, Limited Data Retention, Ethical Practice, Data Ownership and Control.* The Strong level of Concordance *(W)* from the experts indicates that the experts believe that the implementation of these measures will provide privacy and assurance during utilization and interaction with various IoT and social media platforms. Industry experts are also deeply concerned that privacy breaches might trigger social insecurity among end-users, thereby reducing consumer interactions with IoT devices and social platforms, triggering a need to completely stay away from IoT devices and social platforms. This reinforces the views of privacy advocates that ensuring privacy and adequate personal data protection for users is extremely fundamental to individual safety in a digital environment.

6. Discussion of Findings and Conclusions

Consumer data is both an economic asset and a personal right. Privacy rights have evolved from a legal afterthought to a *cornerstone of digital trust*, governance, and legitimacy. Robust policy frameworks, ethical governance, technical safeguards, and organizational accountability are indispensable to protect privacy while enabling innovation. Achieving this balance requires *multi-stakeholder engagement*, harmonized regulation, and a shift toward human-centered digital ecosystems where individuals retain agency over their data. A consensus of opinions from industry experts on best practice measures to help protect consumer privacy in a digital age. The right to privacy is a fundamental right and foundational for the healthy development of self and community. Data mining has become an indispensable component of the digital economy, yet its expansion has fundamentally altered the balance between innovation, privacy, and individual autonomy. The

 doi:10.20944/preprints202606.1262.v1

digital age demands a re-examination of how data is governed, how consent is operationalized, and how autonomy is preserved in increasingly automated and data-driven environments. Addressing these issues requires interdisciplinary inquiry, combining insights from technology, law, ethics, behavioral science, and organizational governance. Findings from the study indicate that industry experts are unanimous on privacy concerns. A dynamic Kendall's *Coefficient of Concordance (W)* was used to determine the level of Concordance on the proposed privacy measures in a digital environment. The research showed a strong consensus amongst industry experts on the effectiveness of the following privacy measures: *Privacy-By-Design (PBD), Strong Privacy Protection Laws and Enforcement, End-To-End Encryption, Third-Party App Permission, User-Friendly Privacy control settings, Data Minimization, and Data Ownership & Control.* Participants believe these measures would have a significant impact when implemented as privacy-preserving measures. *Privacy-by-design concept,* as a privacy-preserving measure, involves designing the features that allow privacy features to be embedded into the architectural framework of the IoT media platform in a digital environment. *Data minimization* prioritizes data collection to be minimized to only what is necessary for the platform's functionality. This limits the collection and retention of consumer data to only functional purposes. The study adds to the existing body of knowledge on the need preserve preserving privacy in a digital environment, and enhances privacy through the implementation of effective privacy-preserving measures. The major privacy and autonomy litigation issues in recent years have significantly highlighted the need for broader transparency and oversight amongst digital companies. Such as Cambridge Analytica and Meta-Facebook (Unauthorized Data Harvesting); Google Location Tracking Cases (Germany and US), TikTok and Minor Privacy Cases (Child Data Protection), Apple App Tracking Transparency (ATT) and Legal Pushback, Amazon Alexa and Smart Speaker Surveillance. In many jurisdictions, courts have become key arenas for adjudicating these disputes, highlighting gaps in legal protection, corporate practices, and public expectations regarding privacy and autonomy [6]. This recent wave of privacy litigation—against these technology giants *Meta* (Facebook), *Google, Apple, TikTok, and Amazon*—reveals a broader societal and legal reckoning over *consumer data, privacy rights, and autonomy* in digital environments. Privacy advocates with the Courts are increasingly demanding that digital companies provide *transparent, specific, and user centric* explanations of data collection and use, that meaningful choice and control be embedded in consent mechanisms, and that data-driven systems respect individual autonomy rather than undermine it. Going forward, digital firms will need to institutionalize privacy and autonomy as core design, governance, and strategic priorities. Litigation and regulatory trends make it clear that data transparency is no longer a competitive differentiator—it is a *legal imperative and a foundation of digital trust.*

7. Future Research

The convergence of data mining, consumer privacy, and autonomy represents one of the most critical challenges of the digital age. While data mining continues to drive innovation and economic growth, its unchecked application risks undermining fundamental rights and ethical norms. Understanding how data mining practices affect consumer privacy and autonomy—and how policy, governance, and organizational strategies can mitigate these effects—is essential for developing sustainable, trustworthy digital ecosystems. An area of future study that might be further explored through additional research is the effect and impact of privacy concerns on antisocial behavior and social insecurity in a digital environment. Individuals strive to constantly protect their privacy to ensure their data is being used responsibly in ways consistent with established laws and norms, and would not violate their rights. The study demonstrated the significance and importance of privacy-preserving measures in a digital environment and added to the general body of knowledge by providing effective privacy-preserving measures to help enhance consumers' privacy in a digital society, to allay the fears and privacy concerns of consumers that can influence and shape interaction with digital devices in a digital age. Future research is required to better understand the relationship

 doi:10.20944/preprints202606.1262.v1

between privacy concerns and anti-social behavior and interactions in a digital age, which helps to increase consumer trust and interaction with digital technologies in a digital environment.

Funding: This work is not supported by any external funding.

Data Availability Statement: The data supporting the outcome of this research work has been reported in this manuscript.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

APP:	Australian Privacy Principles
CAN-SPAN	Control Assault of Non-Solicit Pornography and Marketing Act2003
CCPA	California Consumer Privacy Act
CFAA:	Computer Fraud & Abuse Act of 1986
COPPA	Children's Online Privacy Protection Act Of 1998
DM	Data Mining
ECOA:	Equal Credit Opportunity Act
ECPA:	Electronic Communication Privacy Act
EFTA:	Electronic Fund Transfer Act
FACTA:	Fair and Accurate Credit Transactions Act of 2003
FTC:	Federal Trade Commission
FCRA:	Fair Credit Reporting Act
FDCPA:	Fair Debt Collection Practice Act
GDPF:	General Data Protection Regulation
GLBA:	Gramm-Leah-Bliley Act
HIPAA:	Health Insurance Portability and Accountability Act
IOT:	Internet of Things
IT:	Information Technology
LGPD:	General Personal Data Protection Act
NIST:	National Institute of Standard and Technology
PII:	Personal Identifiable Information
PIPEDA:	Personal Information Protection and Electronic Documents Act
PPI:	Protection of Personal Information Act Japan
POPIA:	Protection of Personal Information Act Argentina
PDPA:	Personal Data Protection Act
RTBF:	Right TO BE Forgotten

References

1. ACLU (2014). Privacy rights in the digital age. American Civil Liberties Union Foundation, OHCHR, 19(1), 1-41. https://www.aclu.org
2. Aggrawal, C. & Yu, P. S. (2008). A general survey of privacy-preserving Data mining Models and algorithms, In privacy-preserving data mining. Models and Algorithms, *34*(1), 1-2. http://charuaggarwal.net/generalsurvey.pdf
3. Almutairi, N. M. (2020).Privacy-preserving third-party Data mining using Cryptography.ProQuest LLC Dissertation, #29081972, 1-241.
4. Andre, Q., Carmon, Z., Wertenbroch, K. and Crum, A. (2018). Consumer choice and Autonomy in the age of intelligence and big data. Customer Needs and Solutions, 1(5), 28-37. https://doi.10.1007/s40547-017-0085-8
5. Ajah, I.A and Nweke, H. F. (2019). Big data and business analytics: Trends, platforms, Success factors, and applications. Big Data and Cognitive Computing, *3*(32), 1-32. https://doi.10.3390/bdcc3020032
6. Babu, P. N. & Ramakrishna, S. (2020). Critical review of privacy and security issues in Data mining. Emerging research in Data Engineering Systems and Computer Communications, *2*(1), 217-230. https://doi.10.1007/978-981-15-0135-7_21

 doi:10.20944/preprints202606.1262.v1

7. Becker, B. W. (2018).Information literacy in the digital age: Myths and Principles of Digital literacy. School of Information Student Research Journal, 7(2), 1-10. https://scholarworks.sjsu.edu/ischoolsrj
8. Bjorlo, L., Moen, O. & Pasquine, M. (2020). The role of consumer autonomy in Developing sustainable AI. A conceptual framework: Sustainability, 2(13), 1-18. https://doi.org/10.3390/su13042332
9. Biswas, S., Khare, N., Agrawal, P., & Jain, P. (2021). Machine learning concepts for correlated big data privacy. Research Square, *1*(1), 1-22. https://doi.10.21203/rs.3.rs388753/v1
10. Bulger, M., McCormick, P., & Pitcan, M. (2017). The legacy ofInbloom:Data&Society.WorkingPaper,1-34. https://datasociety.net/pubs/ecl/InBloom_feb_2017
11. Cao,Y., Wei,W., Zhou,J.,(2022). Privacy protection datamining algorithm in Blockchain Based on decision tree classification.20 (2). https://doi.org/10.3233/WEB-210485
12. Carmon, Z., Wertenboch, K., & Yang, H. (2020, February 28). Consumer autonomy Violations and the coming AI Backlash. The business school for the world. https://knowledge.insead.edu/marketing/Consumer-autonomyviolations-and-the-comingai-backlash
13. Chan, K, (2024, January 29). Amazon scraps 1.7 Billion deal to buy Roomba maker iRobot after EU antitrust resistance. Tech Antitrust. The Associate Press, https://fortune.com/europe/2024/01/29/amazon-iRobot-eu-antitrust-1-7-billion-dealscrapped-roomba/
14. Chen, M., Tian, G., and Tao,Y. (2023). Data Mining Algorithm of experimental sports marketing Based on cloud computing technology. Journal of Computational Methods in Science and Engineering. 23(6). 3315-3330. https://doi.org/10.3233/JCM-226908
15. CMA (2021, January 19). Algorithms: How they can reduce competition and harm Consumers, Competition &Market Authority, www.gov.uk/cma
16. CMA (2023). Anticipated acquisition by Adobe Inc. of Figma, Inc.Competition & Market Authority, 1-2. www.gov.uk/cma
17. Collins, D. (2022, November 14). Google reaches 391.5m settlement with 40 US States Over location Tracking. Associated Press.https://www.irishexaminer.com/world/arid41006543.html
18. Congressional Research Services CRS (2023) Cyber Crime and the Law: Primer on the Computer Fraud and Abuse Act and Related Status.1-56 https://crsreport.congress.gov
19. CRS (2012) Privacy: An Overview of the Electronic Communication Act: Congressional Research Services, 1-90.R4173. https://crsreport.congress.gov
20. Darwish,S. M., Essa, R. M., Osman, M. A., and Ismail, A. A. (2022). Privacy Preserving Data Mining Framework Negative Association Rules: An Application to Healthcare Informatics. IEEE Access.10. 1-13, https://doi.org/10.1109/ACCESS.2022.3192447
21. Deloitte (2017). Security and privacy in the digital world Deloitte Touche Tohmatsu India LLP: Confederation of Indian, 1-27. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/security-and-privacy-noexp.pdf
22. Demertzis,M. (2021,February 02).Strategic autonomy or Strategic alliance? Bruegel,https://www.bruegel.org/comment/strategic-autonomy-or-strategic-alliance
23. Denker, A. (2021). Protection of privacy and personal data in the big data environment Of smart cities. The International Archives of the Photogrammetry, Remote Sensing andSpatial Information Sciences. 46(4), 181-186. https://doi.org/10.5194/isprs-archives-XLVI4-W5-2021-181-2021
24. DeSmet, C. & Diane J. C. (2019). Recent developments in privacy-preserving mining Of clinical data. ACM/IMS Trans. DataSci, 2(4), 1-32. https://doi.dl.acm.org/doi/pdf/10.1145/3447774
25. European Commission (2020,December 20).Antitrust: Commission accepts Commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to BuyBox and Prime. Press Corner. Brussels. https://ec.eutropa.eu
26. Ekaputra, F. J., Ekelhart, A., Mayer, R.,Miksa, T., Sarcevic, T., Tsepelakis, S., Waltersdorfer, L. (2024). Semantic-enabled Architecture for Auditable Privacy-Preserving Data Analysis.SemanticWeb.15(3).675-708. https://doi.org/103233/SW-212883
27. Federal Register (2024). Children's Online Privacy Protection Rule. Federal Trade Commission. Federal Trade Commission.The Daily Journal of the United States N 3084-AB20.https://www.regualtions.gov

 doi:10.20944/preprints202606.1262.v1

28. Froomkim, M. A. (2000). The death of privacy. Stanford Law Review, Symposium: Cyberspace and Privacy. A new legal paradigm, 52(5), 1461-1543. https://doi.org/10.2307/1229519
29. Galvin, K. H. and Demuro, P. R. (2020).Developments and privacy and data ownership in Mobile health technologies 2016-2019 National Library of Medicine, 29(1), 32- 43. https://doi.org/10.1055/s-0040-1701987
30. Gal, M. S. (2018). Algorithmic challenges to autonomous choice. Michigan Technology Law Review, 25(1)60 -104. https://repository.law.umich.edu/mttlr
31. Grant, N. (2023, December 13) Google loses antitrust court battle with makers of Fortnite Video game. International Business News, The-Times-of-India. https://www.nytimes.com/2023/12/11/technology/epic-games-google-antitrustruling.html
32. Guennoun, M., & Mouftah, H. T., Youssef, G. (2016). Big data analytics: Security and Privacy challenges. IEEE Symposium on Computers and Communication (ISCC) https://doi.10.1109/ISCC.2016.7543859
33. Goldstein, K., Tov, D., Ohad, S & Prazeres, D. (2018). The right to Privacy in the Digital Age. Pirates Parties International, 1(2), 1-8. https://www.researchgate.net/publication/328789396
34. Hamms, J. (2020).Preserving privacy of continuous high-dimensional data with Minimax Filters. International Conference on Artificial Intelligence, 1-9. https://www.cs.tulane.edu/jhamma/papers/aistats15_2_jh_final.pdf
35. Harripaul, K. (2021). Information privacy in an age of invisible shopper tracking: who will pay the price for stores of the future? Georgia State University Law Review, 37(3), 1077–1123. https://readingroom.law.gsu.edu/gsulr/vol37/iss3/10/
36. Hoffer, R. (2019). Austrian competition law: Tough on big-tech. Competition Law International, 15(2), 131 -137, https://search.ebscohost.com
37. Hong-Yen, T., & Jiankun, H. (2019). Privacy-preserving big data analytics a Comprehensive survey. Journal of Parallel and Distributed Computing.1(134), 207-218. https://doi.org/10.1016/j.jpdc.2019.08.007
38. Hunton, A. K. (2021). Data protection & privacy: Leaders in privacy and cybersecurity, Law Business Research, 1(2), 1-18 https://www.lexology.com/gtdt
39. Hua, X., and Zhang, H. (2024), International Trade Privacy Data Management System, Combining Internet-of-things. Intelligent Decision. Technologies, 18(1), 211-22, https://doi.org/10.3233/IDT-230393
40. InFocus (2022). Data protection and privacy law: An introduction: Congressional Research Service CRS. 2(1), 1-3. https://crsreports.congress.gov
41. IFLA (2018). The right to privacy in the digital age. The International Federation of Library Associations and `Institutions.1-5.https://cdn.ifla.org/wp-content/uploads/files/assets/faife/ochr_privacy_ifla.pdf
42. ISACA (2020). Privacy Compliance –A path to increase trust in technology.The-Practical-Aspect,ISACAJournal, 1(6), 15-19 https://www.isaca.org/resources/glossary#glossp
43. Iwan, D. (2021). Application of human rights control mechanisms in algorithms Decision-making cases, Licenciado sob Uma Licença creative commons, 26(2), 269-291. https://doi.org/10.25192/issn.19820496.rdfd.v26i22286
44. Jin, G. Z. (2018) Artificial Intelligence and Consumer Privacy. NBER Working Papers.1-25. https://www.nber.org/papers/w24253
45. Katharine, D. (2020). Introduction: Regulation and oversight of digital campaigning: Problems and solution: Academic Journal. 91(4), 705-712. https://doi.org/10.1111/1467-923X.12888
46. Kelly, M. J. and Satola, D. (2017). The right to be forgotten.University of Illinois law Review, 2017(1), 1-64. https://ssrn.com/abstract=2965685
47. Keen,C. (2020). Apathy, Convenience or Irrelevance? Identifying Conceptual Barriers to Safeguarding Children's Data Privacy. 24(1), 50-69. https://doi.org/10.1177/1461444820960068
48. Lett, M. (2020). Autonomy in consumer choice. PMC US national library of medicine National Institute of Health, 1(8) 1-11. https://doi.10.1007/s11002-020-09521-z
49. Lv, L., Yang, Z., Zhang, L., Huang, Q., & Tian, Z. (2021). Multi-party transaction Framework for drone services based on alliance blockchain in smart cities. Journal of Information SecurityandApplications, 58(4), 1-8. https://doi.org/10.1016/j.jisa.2021.102792

 doi:10.20944/preprints202606.1262.v1

50. Macmillan, R. (2020). Big data, machine learning, consumer protection, and privacy: Security, infrastructure, and trust working group. Financial Inclusive Global Initiative FIGI, 1-62. https://figi.itu.int/wp-content/uploads/2021/04/Big-data-Machine-
51. McIntosh, D. (2019). We need to talk about data: how digital monopolies arise and why they have power and influence. Journal of Technology Law &Policy, 23(2), 185-213. https://scholarship.law.ufl.edu/jtlp
52. Miller,V. (2025). Students Under Surveillance: Big Data Policing and Privacy Rights.Educational Researcher.XX(X), 1-4. https://doi.org/10.3102/0013189X251318346
53. Mittelstadt, B. D., Allo, P., Taddero, M., Wachter, S. & Florida, L. (2016). The Ethics of Algorithms: Mapping the Debate. Big Data & Society, Original Research Article, 1(2), 1-21 https://doi.org/10.1177/2053951716679679
54. Moss. E & Metcalf, J. (2019, November 14). The Ethical Dilemma at the Heart of Big Tech Companies. Business Ethics, Harvard Business Review HBR. https://hbr.org/2019/11/the-ethical-dilemma-at-the-heart-of-big-tech-companies
55. Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computer and Society, 27(3), 27-32. https://doi.org/10.1145/270858.270866
56. Murugeshwari, B., Selvaraj, D., Sudharson, K., Radhika,S. (2023),Data Mining with Privacy Protection Using Precise Ecliptical Curve. Intelligent Automation & Amp; Soft Computing.35(1), 839-851. http://doi.org/10.32604/iasc.2023.028548
57. Nissenbaum, H. (2004). Privacy as contextual integrity: Washington law review, 79(119), 1-8. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10
58. Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of Privacy in public. Law and Philosophy. 17(1), 59-596. https://nissenbaum.tech.corell.edu
59. Nass, S. J., Levit, L. A., & Gostin, L. (2009). Beyond the HIPAA privacy rule: Enhancing Privacy, improving health through research: Institute of Medicine (US) committee on health research and privacy information. The HIPAA Privacy Rule, National AcademicsPress(US). 1-320. https://www.ncbi.nlm.nih.gov/books/NBK9579/#a20016f79ddd00061
60. OECD (2020). The impact of big data and artificial intelligence (AI) in the insurance Sector.OECD, 1-36. https://www.oecd.org/finance/The-Impact-Big-Data-AI-InsuranceSector.pdf
61. Persch, J. (2021). The role of fundamental rights in antitrust law–a special responsibility For undertakings with regulatory power under Art.TFEU?. European Competition Journal, 17(3), 542–566. https://doi.org/10.1080/17441056.2021.1921514
62. Phelps. J.E, Nowak. G. J., & Ferell. E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19(1), 27-41. https://https://doi.org/10.1509/jppm.19.1.27.16941
63. Popescu,M.,Baruh,L.,Sudhakar,S. (2024). Role-based Privacy-Cynicism and local privacy Activism: How Data Stewards Navigate Privacy in Higher Education. Big Data &Society. 11(2). https://doi.org/10.1177/2053951724120664
64. Rafiq,F.,Awan,M. A.,Yasin,A.,Nobanee,H.Zain,M. A., Bahaj, S. A. (2022).Privacy Prevention of Big Data Applications: A Systematic Literature Review. 12(2), 1-23. https://doi.org/10.1177/21582440221096445
65. Raul, A. C. (2021). Privacy, data protection, and cyber security law review. The law Reviews, 1(8), 1-47. https://www.sidley.com/en/-/media/publications/the-privacy-data protection-and-cybersecurity-law-review-2021-us
66. Rao, P. R.M., Krishna, S. M. & Kumar, A. P.S. (2018). Privacy preservation techniques in Big data analytics: A Survey. Journal of big data,5(33),1-12. https://doi.org/10.1186/s40537-018-018-0141-8
67. Raval, V., & Shah, S. (2020). The practical aspect: Privacy compliance-A path to Increase trust in technology. Privacy. The Practical Aspect. 6, ISACA. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/privacy-compliancea-path-to-increase-trust-in-technology
68. Romansky, R. (2021). Privacy and data protection in the contemporary digital age.United Nations High Commissioner for Human Rights International Journal on Information Technologies & Securities. 13(4), 1-12. https://ijits-bg.com/contents/IJITS2021-No4/2021-N4-09.pdf

 doi:10.20944/preprints202606.1262.v1

69. Rosner, G., and Kenneally (2018). Privacy and the Internet of Things: Emerging Frameworks for policy and design. Center For Long-Term Cybersecurity. 1-28. https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf
70. Rosoff, M. (2021, June 30). This week shows how the big tech antitrust campaign is Misguided. CNBC Tech Op-Ed. https://www.cnbc.com/2021/06/30/op-ed-antitrustcrusade-against-Big-tech-is-misguided.html
71. Romansky, R. P., and Noninska, I. S. (2020). Challenges of the digital age for Privacy and Personal data protection, Mathematical Biosciences, and Engineering, 17(5), 5288-5303. https://doi.10.3934/mbe.2020286
72. Richards, N. & Hartzog, W. (2016). Taking trust seriously in privacy law. Stanford Technology Law Review, 1(19), 431- 472. https://doilaw.standford.edu
73. Saifan, A. A., and Lataifeh, Z. (2021). Privacy- Preserving Defect Prediction Using Generalization And Entropy-based data reduction. Intelligent Data Analysis. 25(6), 1369-1405. https://doi.org/10.3233/IDA-205504
74. Shah, A. & Gulati, R. (2016) Privacy-preserving data mining: Techniques, classification, and Implications – A survey. International Journal of Computer Applications, 137(12) 40-46. https://doi.org/10.5120/ijca2016909006
75. Shoba, V. & Srinivan, S. (2018). Privacy-preserving big data analytics-A review. International Journal of Pure and Applied Mathematics, 119(15), 2825-2832. https://acadpubl.eu/hub/2018-119-15/2/300
76. Smahi, A., Xia,Q., Xia,H. Suleimana, N. Fateh, A. A., Gao, J., Du, X., Guizan, M. (2020). A Blockchainized privacy-preserving support vector machine classification on mobile crowd-sensed data. Perversive and Mobile Computing, 66(2020), 1-18. https://doi.org/10.1016/j.pmcj.2020.101195
77. Srijaynthi, S. & Sethukkarasi, R. (2017). A comprehensive survey of privacy-Preserving big Data Mining. International Journal of Computer Applications Technology and Research, 6(2), 79-86.https://ijcat.com/archives/volume6/isue2/ ijcatr06021002.pdf
78. Strycharz, J. & Duivenvoorde, B. (2021).The exploitation of vulnerability through Personalized marketing communication: are consumers protected? Internet Policy Review, 10(4), 1-27. https://doi.org/10.14763/2021.4.1585
79. Stuart, T. (2021). Too little too late? An exploration and analysis of the inadequacies of Antitrust law when regulating GAFAM data-driven mergers and the potential legal remedies available in the age of big data. European Competition Journal, 17(2), 407–436. https://doi.org/10.1080/17441056.2021.1909234
80. Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and Manipulation.Journal on Internet Regulation, 8(2), 1-22. https://doi.10.14763/2019.2.141/
81. Shuham, M. (2019, November 21). Sacha Baron Cohen calls out "Ideological Imperialism" of social Sites boosting.TalkingPointMemoTPM. https://talkingpointsmemo.com/news/sacha-baron-cohen-calls-out-ideological-imperialism-of-social-sites-boosting-hate
82. Tang, A. (2023) Privacy In Practice: Establish and Operation a Holistic Data Privacy Program. CRC Press.1st Ed.1-471. https://doi.org/10.1201/9781003225089
83. Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate Online privacy policy. Methaphilosophy LLCandBlackwellPublishingLtd, 38(1), 1-22. https://www.jstor.org/stable/24439672
84. Tavani, H. T. and Moor, J. H. (2001). Privacy protection, con-trol of information, and Privacy-enhancing technologies.ACMSIGCAS Computers and Society, 31(1), 6-11. https://doi.org/10.1145/572277.572278
85. Taschner, J. (2021). Era of Accelerating Digital Convergence: Security, Surveillance, Data, Privacy, Big Tech, and Politics. AM. U.INT'LL.REV., 36(4), 773-845. https://digitalcommons.wcl.american.edu
86. Telikani, A., Shahbahrami, A., & Gandomi, A. H., (2021). High-Performance Implementation of evolutionary privacy-preserving algorithm for big data Using GPU platform. Information Sciences, 1(579), 251-265. https://www.sciencedirect.com
87. Turley, J. (2020). Anonymity, obscurity, and technology: Reconsidering privacy in the Age of biometrics. Boston University Law Review, 100 (6), 2179-2261.
88. Tran, H. Y. and Hu, J. (2021). Privacy-preserving big data analytics a comprehensive Survey.Journal of parallel and distributedComputing, 134(1), 207–218. https://doi.org/10.1016/j.pdc.2019.08.007

 doi:10.20944/preprints202606.1262.v1

89. Ulrike, S.F, Marquardt, K., Golowko, N., Kompalla, A. and Hell, C. (2018). Digital Transformation and its Implications on Organizational Behavior. Journal of EU Research in Business, 20(18), 1-14. https://doi.org/10.5171/2018.340873
90. Virupaksha, S. and Dondeti, V. (2021) Anonymized noise addition in subspaces for Privacy preserved data mining in high dimensional continuous data. Peer-to-Peer Networking and Applications,14, 1608-1628. https://doi.org/10.1007/s12083-021-01080-y
91. Wasastjerna, M. C. (2018).The role of big data and digital privacy in merger review. European Competition Journal, 14(3), verification algorithm based On data mining and accounting information.ScientificProgramming, 1(2022), 1-11. https://doi.org/10.1155/2022/475899
92. Weber, R. H. (2011). The Right to be forgotten: More than a pandora's box? JIpItec,1-11. http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8
93. Wertenbroch, K., Schrift, R. Y., Alba, J. W., Barasch, A., Bhattachajee, A. Giesler, M., Knobe, J., Lehmann, D. R., Matz, S., Gideon, N., Jeffrey, R. P., Puntoni, S., Zheng, Y. & Zwebner, Y. (2020). Autonomy in consumer choice. Springer Link, 31(1),429-439.https://link.springer.com/article/10.1007/s11002-020-09521-z
94. Woodrow, H., Evan, S., Johanna, G. (2024). Privacy Nicks: How the Law Normalize Surveillance.Washinghton University Law Review. 101(717) 1-74.
95. Yang, X. Kelarev, A., Yi, X. (2024). Privacy-enhancing data aggregation and data analytics in Wireless networks for a large class of distributed queries. Wireless Network. 30. 4749-4759
96. Yuan,Y., Xu, H., M. Krishnamurthy, M., and P. Vijayakumar (2024).Visualization Analysis of Educational Data Statistics Based on Big Data Mining. Journal of Computational Methods in Sciences and Engineering. 24(3), 1785-1793. https://doi.org/10.3233/JCM-230003
97. Yue, L. (2024). E-Commerce Return Data Based on Frequent itemset Mining and time Series Symbolization Clustering Journal of Computational Methods in Science and Engineering. *25*(3) 1-16. https://doi.org/10.1177/1472798241309189
98. Zhang, L., Huo, Y., Ge, Q., Ma, Y., Liu, Q., & Ouyang, W. (2021). A privacy Protection Scheme for IoT big on time and frequency limitation. Wireless Communication And Mobile Computing, 1(2), 1-10. https://doi.10.1155/2021/5545648