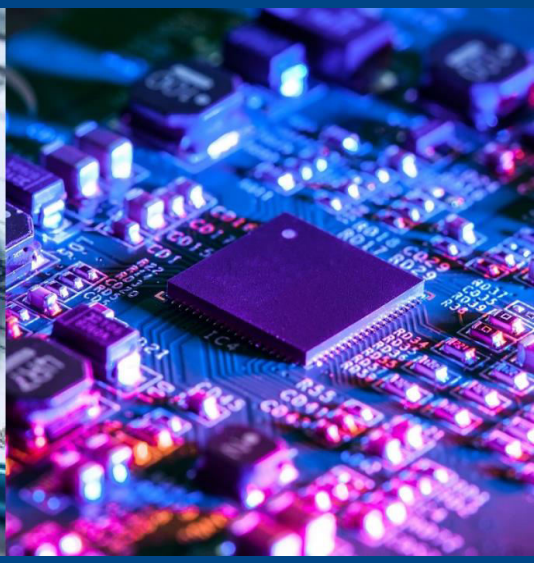
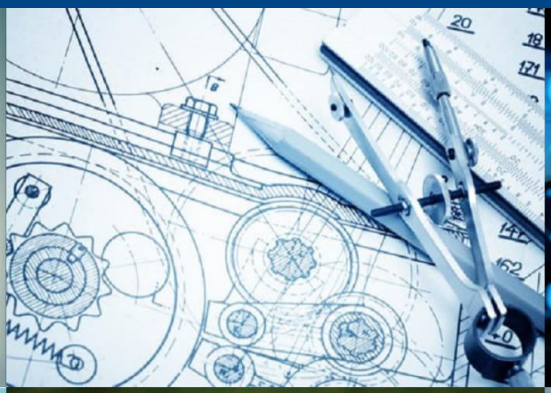
ISSN: 2582-7219

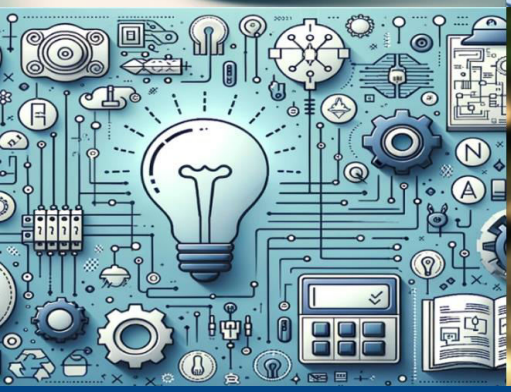




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904483

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

How IT Professionals Describe Innovative Strategies to Monetize Data in the Context of Data Privacy

Michael Abisa, John Kuhn

Grand Canyon University, Phoenix, Arizona, United States

Purdue Global University, West Lafayette, United States

ABSTRACT: The researchers explored how IT Professionals describe innovative strategies to monetize data in the context of data privacy in the United States. The overarching research question was: How do IT Professionals describe the risks and benefits of innovative strategies to monetize data in the context of data privacy? The theoretical foundation was Laufer and Wolfe's privacy calculus theory. The sample comprised IT professionals from data privacy groups (IAPP), LinkedIn, and Facebook who reside in the United States. Data collection for this qualitative descriptive design included a demographic questionnaire, semi-structured interviews, and focus groups. Data analysis included descriptive statistics, thematic analysis, and a description of the phenomenon. The researchers identified six key themes. The Data Security and Breach Prevention, Emerging Data Collection Technologies, Preventing Emerging Threats to Consumer Data Privacy, Responsible Data Monetization, Data Privacy Control, and Data Consent and Transparency.

KEYWORDS: Data monetization, data privacy concerns, privacy violation, data breaches, innovative strategies, data privacy risk, blockchain, data minimization, hacker, California Consumer Privacy Act, General Data Protection Regulation

I. INTRODUCTION

The emergence of data monetization business models highlights the importance of access control, authorization, and confidentiality in the modern data economy. The economic value of consumers' personal data has increased the collection of consumers' personal information for quantifiable benefits. Previous studies have emphasized the need to understand how data-driven innovation affects user privacy (Saura et al., 2021), noting that consumers often freely provide their data to companies that then fail to act as responsible custodians (Harris, 2020). In today's data economy, protecting sensitive information is crucial.

The data monetization business model allows business organizations to collect, store, and monetize consumers' personal data. Ray et al. (2020) reported that there is an increasing awareness among business organizations that their enterprise data holds significant value for other organizations in making major business decisions. Zhang et al. (2023) noted that content providers and media organizations sometimes sell consumer data to advertising companies for targeted advertising purposes. For example, Facebook generates revenue by providing data about its users on the social network platform to advertisers (Quach et al., 2022). Given that several business organizations, including Target (Alder, 2024), have experienced data breaches in recent years, and given that there are growing concerns about consumers' data privacy (Martin, Kim, Palmatier, et al., 2020), business organizations need to implement strong data security measures.

To foster trust and secure information disclosure, it is paramount to protect customers' data privacy. Providing adequate data privacy and security can help reduce organizational data breaches. Data privacy is a critical concern in data monetization. The researchers extensively explored innovative strategies for IT professionals to balance data monetization goals with the safeguarding of user privacy. Existing research has focused more on the business or organizational aspects of data monetization rather than specifically examining the perspectives and experiences of IT professionals who play a crucial role in designing and implementing innovative data collection, storage, and sharing or selling consumer data.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

Data monetization and consumer data privacy are major concerns for business organizations and consumers. Recognizing data monetization as the conversion of intangible data value into tangible benefits, it is essential to acknowledge the growing concerns about data privacy due to frequent data breaches and the emergence of data privacy laws, such as GDPR and CCPA. Addressing consumer data privacy concerns requires identifying innovative tools to monetize consumer data while preserving their data privacy.

The researchers investigated how information technology (IT) professionals describe the risks and benefits of innovative data monetization strategies to monetize data in the context of data privacy in the United States. Baecker et al. (2020) conducted a study on business strategies for data monetization, identified various ways organizations monetize data, and recommended future studies to explore innovative ways to monetize data in the context of data privacy. Parvinen (2020) noted that "data monetization models through selling data to third parties have received less attention in the academic literature, and the few studies that do focus on the issue operate at the conceptual or anecdotal case study level" (p. 26). The researchers conducted a literature review that covered personal data as a strategic asset, data privacy concerns, and relevant data privacy regulations.

III. PERSONAL DATA AS A STRATEGIC ASSET

In today's data-driven landscape, business organizations are increasingly recognizing the immense value of enterprise data, particularly personal data, as a strategic asset. According to Kathoke et al. (2022), the global data monetization market was valued at $2.1 billion in 2020 and is projected to reach $15.4 billion by 2030, growing at a compound annual growth rate (CAGR) of 22.1% from 2021 to 2030. As businesses and governments leverage consumer personal data for economic gains (Han et al., 2020) and targeted decision-making (Duan et al., 2022), consumers' personal data has become vulnerable to data privacy. The rise of digital technologies like Big Data analytics, artificial intelligence (AI), and machine learning has transformed data monetization into a new business model, allowing business organizations to collect, analyze, and store vast amounts of consumers' personal data to gain a competitive advantage.

The potential economic value of personal data makes it a tremendous organizational asset. Wixom et al. (2021) voiced that most global companies aim to treat data as a strategic asset. As a result of economic value in consumers' personal data, it has become a strategic asset for businesses and government agencies in the current data economy. However, Birch et al. (2021) noted that standardized corporate accounting practices do not recognize digital personal data as an asset on balance sheets. Therefore, quantifying the value of personal data may create difficulty for organizations, as they do for traditional (tangible and intangible) assets. Organizations and various stakeholders can collaborate to identify how to recognize it as an asset on balance sheets.

IV. DATA PRIVACY CONCERNS

The increasing collection of consumer data, driven by technological advancements, has heightened privacy concerns, necessitating a balance between business innovation and individual data rights. Organizations can use novel touchpoint technologies like location tracking or facial recognition to gather consumers' data invisibly without the consumer's permission (Martin & Palmatier, 2020). Krafft et al. (2021) revealed that such privacy concerns have led government agencies such as the FTC to regulate fair data collection and usage by requiring online companies to explicitly inform consumers of the data collected by the firms and how the data will be used. Collecting consumers' personal data without their consent can pose a huge risk to their privacy. Research by Han et al. (2020) demonstrated that even anonymized data can be de-anonymized when combined or linked to other sources.

To address consumers' data privacy concerns, businesses must prioritize ethical data collection practices, ensuring transparency, obtaining explicit consent, and building trust with consumers. Integrating ethical principles into all organizational operations, from leadership to software development, is crucial for fostering a secure and equitable digital environment where consumer privacy is protected.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904483

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. DATA PRIVACY REGULATIONS AND LAWS

The EU's GDPR and California's CCPA are leading data privacy laws, aiming to regulate how organizations collect and use personal information while granting data subjects control over their data. Using appropriate technology to address privacy concerns would require ethical deliberation and responsibility. Individual states in the U.S. have adopted regulatory actions to protect their consumers' data (Klaus & Elzweig, 2020). For example, California has data privacy and personal data protection laws like the GDPR, but this protection is only limited to the state of California (Line et al., 2020). Fefer and Archick (2021) remarked that in the U.S, data privacy has traditionally been regulated at a sectorial level to protect specific data types. U.S. policymakers can work with all stakeholders to develop federal data privacy regulations similar to the GDPR, which may include all the different sectorial-level privacy regulations.

In the absence of federal privacy laws in the U.S., California has enacted data protection regulations for its residents. The CCPA gives consumers more control over the personal information collected by businesses (Rothstein & Tovino, 2019). The GDPR and CCPA are becoming the global standards for data privacy and protection because of the number of citizens they protect (about 508 million in the E.U. and about 35.9 million California residents, respectively) and the broad application of the law to many companies (Barrett, 2019). Therefore, the GDPR and the CCPA may serve as reference guides for other countries and jurisdictions that want to create standard data privacy regulations to protect their citizens.

There are some categories of data that the CCPA may not apply, such as already-protected medical information and certain publicly available information. The application of CCPA does not include protected health information collected by covered entities and business associates regulated by the HIPAA Privacy Rule (Rothstein & Tovino, 2019). Despite some federal sector-specific laws like HIPAA, the U.S. lacks a comprehensive federal data privacy law, making the CCPA a significant state-level regulation, although enforcement through agencies like the California Attorney General's office faces issues such as broken or missing "Do Not Sell" links on websites (O'Connor et al., 2021). To help increase compliance with the CCPA, regulatory agencies should conduct random tests on organizations' websites to see if they abide by the policy.

VI. METHODOLOGY

The researchers conducted a qualitative descriptive study to understand how IT professionals perceive the risks and benefits of innovative data monetization strategies in the context of data privacy in the United States. Ofulue and Benyoucef (2024) stated that organizations aspiring to monetize their enterprise data effectively need to understand various data monetization models, their implications, opportunities, and limitations. Recognizing a gap in existing literature on this emerging field, the researchers sought perspectives from IT professionals who build data platforms. The Researchers contacted IT professionals from data privacy organizations like the International Association of Privacy Professionals (IAPP) and used professional networks like LinkedIn and Facebook to recruit participants for a focus group and individual interviews. The study's design focused on providing a comprehensive description of these professionals' insights into balancing data monetization with consumer data privacy.

In recent years, there has been a growing interest in developing innovative strategies or practical ways to monetize data while addressing data privacy concerns. This interest is reflected in the research of Baecker et al. (2020 who highlighted the need for further research in this area. Therefore, the researcher addressed the identified problem space by researching how IT professionals describe the risks and benefits of innovative strategies to monetize data in the context of data privacy in the United States.

The researchers investigated the perspectives of IT professionals on the risks and benefits of innovative data monetization strategies, guided by the privacy calculus theory. Data was collected from 24 IT professionals (12 in a focus group and 12 in individual interviews) recruited from LinkedIn and Facebook data privacy groups. Participants described their views on the risks and benefits of data monetization in the context of data privacy, with all sessions conducted online (on Zoom and Microsoft Teams) and audio-recorded to gather primary data directly from the participants.

The researchers gathered data from three sources to understand IT professionals' perspectives on innovative data monetization strategies and consumer data privacy. First, a demographic questionnaire identified participants who met

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

the inclusion criteria. Second, two online focus groups, each with six participants, provided in-depth insights into thoughts, feelings, and understanding. Finally, 12 participants were selected for individual semi-structured interviews conducted online using Zoom and Microsoft Teams, allowing for detailed follow-up questions and the exploration of specific themes. Both the focus group and interview questions were developed with expert panels and refined through a field test, ensuring their alignment with the research questions. The study adhered to established interview protocols and maintained trustworthiness through credibility, transferability, dependability, and confirmability

VII. DATA ANALYSIS AND RESULTS

The researchers utilized thematic analysis with inductive coding to analyze the collected data. While complete data saturation was not achieved with 24 participants, the researcher gathered sufficient data to answer the research questions. Eighteen sub-themes emerged from the merged codes, coalescing into six main themes that provided a concise understanding of the IT professionals' perspectives. These themes were systematically organized and presented in tables, including their explanations and supporting participant quotes. Each theme directly addressed one of the two main research questions:

Themes by Research Question

Research Questions	Identified Themes by Research Question
RQ1: How do IT professionals describe the risk of innovative strategies to monetize data in the context of data privacy?	RQ1-T1: Data security and breach prevention RQ1-T2: Preventing emerging threats to consumer data privacy RQ1-T3: Emerging data collection technologies
RQ2: How do IT professionals describe the benefits of innovative strategies to monetize data in the context of data privacy?	RQ2-T1: Data privacy controls RQ2-T2: Responsible data monetization RQ2-T3: Data consent and transparency

Risks of Innovative Data Monetization Strategies (RQ1)

IT professionals identified three primary risks associated with innovative data monetization strategies: data security and breach prevention, emerging data collection technologies, and preventing emerging threats to consumer data privacy**.** Identity theft was described as a high consumer data privacy risk in data sharing and monetization. Participant PC-12 mentioned,

As an engineer, I know that the consumer data privacy risk involves the potential exposure of information that could lead to unauthorized access. For example, the risk is significant if there is identity theft or misuse of data. It also harms the organizational reputation. This can lead to legal consequences. So, that is why whenever we need to create an application, we focus on data privacy risks, which is very important. So, that is my point of view, and by focusing on these areas, AI engineers can mitigate consumer data privacy risks and build trust with users by safeguarding their personal information."

Participant FA-8 added, It is crucial to equip consumers with knowledge and understanding of their data and how they can be protected or have privacy regarding it. So, I believe there have to be ways, and as I said, they involve engaging with people who use these platforms to understand what data privacy is and what they can do themselves.

Ultimately, participants indicated that protecting consumers' identity was essential to reducing their data privacy risk in the digital world. These findings provide insight to help better understand how IT professionals describe the need for innovative strategies to collect and monetize data.

RQ1 Theme 1: Data Security and Breach Prevention: IT professionals emphasized the need for strong security measures to protect sensitive consumer information and maintain trust. They highlighted the importance of continuous monitoring, access controls, and prompt automated responses to data breaches. They also noted that IT and software development teams have a responsibility to report breaches to the appropriate teams for remediation. The IT professionals highlighted the critical role of data monitoring and breach response in protecting consumer data. Participant EH-3 described his organization's 24/7 monitoring system, which quickly detects and responds to threats by

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

disabling affected systems. Participant EH-3 stated, Our monitoring system operates round-the-clock, constantly alerting us to system activities and access to sensitive data.

Participant CA-1, noted the use of monitoring logs and tracking systems to alert administrators to potential issues, allowing for proactive problem-solving, I will say that, you need monitoring loggings, and our company has implemented this whereby we track logs in the user account. Given this, his company has implemented logging systems to track user activity within their account.

RQ1 Theme 2: Preventing Emerging Threats To Consumer Data Privacy: A major risk identified was the potential for data sharing with third parties, which could lead to identity theft and misuse. Many participants had experienced or heard about personal data being exposed on the dark web, making them cautious about data sharing. They emphasized that organizations must be extremely cautious when disclosing consumer data and should utilize transparency and consent to ensure that consumers are aware of how their data will be used and by whom. Participant EH-3 highlighted that his organization actively addresses this by prioritizing data security and system reliability when selecting partners, working closely with their compliance team to ensure regulatory adherence. Similarly, Participant PC-12 emphasized the need for organizations to be extremely cautious when disclosing consumer information to third parties, noting the potential for severe harm to consumers if data is not adequately secured. Participant PC-12 mentioned, Organizations must be extremely cautious when disclosing consumer information to third parties. And you know transparency and communication are crucial; it is essential that, for example, the consumers are aware of how their data will be used and who will access it. A non-disclosure agreement should be made to state the privacy policies and the company regulations.

Participant AM-4 further emphasized the critical importance of obtaining explicit consent from consumers before sharing their data. This is not just a formality, but a vital step towards ensuring transparency and ethical data practices, ensuring that individuals are fully aware of who receives their data, its purpose, and the security measures in place.

RQ1 Theme 3: Emerging Data Collection Technologies: The third theme identified in answering RQ1 was emerging data collection technologies. This theme is defined as how organizations can use technology such as biometrics, encryption, anonymization, and decentralized data storage to enhance consumer data privacy, a topic of utmost importance to the participants. Participants mentioned data masking, anonymization, encryption, and tokenization to describe new technologies to collect consumers' data and protect their privacy securely. They explained that these new methods help protect consumers' data by rendering it unusable or of little value to unauthorized individuals, while allowing authorized personnel and applications to access the data. For example, Participant AH-2 advised organizations to leverage technologies like encryption to help protect consumer data and data anonymity.

Additionally, IT professionals recommended using strategies like data minimization, which involves collecting only the essential data needed for a specific purpose. This approach not only reduces risk but also builds consumer trust and improves operational efficiency.

For example, Participant SB-10 added that consumers are more likely to trust organizations that collect minimal, relevant data, which also makes the data easier to manage, increases operational efficiency, and lowers privacy risks. Participant SB-10 added,

Users are more likely to trust applications that collect only the essential data for their functionality. It is also easy for organizations to handle less collected data, which reduces risk and increases operational efficiency.

Benefits of Innovative Data Monetization Strategies (RQ2)

IT professionals identified three primary benefits of innovative data monetization strategies: data privacy controls, responsible data monetization, and data consent and transparency. Participants consistently emphasized the positive outcomes of robust data privacy practices, including building trust, strengthening customer relationships, mitigating financial and legal risks, and boosting consumer confidence.

RQ2 Theme 1: Data Privacy Controls: IT professionals described data privacy as a fundamental right for consumers. They believe that organizations should provide tools and techniques that give consumers control over their personal data. These techniques include transparent data usage policies, detailed consent options, and user-friendly privacy

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

statements. The participants noted that emerging technologies like blockchain could revolutionize how consumers manage their data, as it offers a decentralized and secure way to take ownership of digital information. By giving consumers more control, organizations can build stronger customer relationships and foster a more privacy-conscious digital environment. Participants AA-9, JR-11, and SB-10 highlighted key strategies for empowering consumers with greater control over their data. For example, Participant JR-11 mentioned, Transparency about data usage and providing detailed consent options can build user trust and compliance with regulations.

Participant SM-5 added, My personal and professional learning is that data privacy is an inherent right for everyone. They have the right to exercise how information about them is consumed, distributed, and made available.

Participant AA-9 pointed to blockchain technology as a revolutionary tool for data privacy. He believes blockchain's inherent decentralization, immutability, transparency, and security features can give individuals true ownership of their digital identities and data, ushering in a new era of control. Again, participant SB-10 stressed the importance of transparent communication in data collection policies.

Participant SB-10 stated, Everything should be mentioned clearly and transparently in the policies. It should be understandable language for common people. Organizations should mention such things in their policies, such as opt-in. For example, if consumers want to share data, they could opt-in, or they should have this as a choice. So, if I'm a consumer who values my privacy, I can just opt out of that.

Organizations can help consumers make informed decisions about their data and foster a more privacy-conscious digital environment by explaining these concepts clearly to consumers in their data privacy policies

RQ2 Theme 2: Responsible Data Monetization: The participants defined this theme as the ethical use of technology to collect and use consumer data. This approach respects privacy, ensures transparency, and provides mutual benefits for both the consumer and the organization. Key strategies included implementing privacy by design principles, which integrate privacy considerations into the development of new systems. They also emphasized the importance of data minimization, which was also a theme for risk mitigation. By collecting only the necessary data, organizations can protect consumer privacy, improve data management, and build a reputation for trustworthiness. Participants SB-10 and SC-11 both emphasized the importance of data minimization for building consumer trust and improving organizational efficiency.

Participant SB-10 stated, Users are more likely to trust applications that collect only the essential data for their functionality. It is also easy for organizations to handle less collected data, which reduces risk and increases operational efficiency.

Participant SC-11 added that organizations or data collectors should collect only the essential data relevant to them to protect consumers' data privacy. She explained that by limiting the amount of personal information consumers collect, organizations can significantly reduce the potential risks to consumer privacy, improve their overall data management practices, and build a stronger reputation for trustworthiness.

RQ2 Theme 3: Data Consent and Transparency: The final theme centered on the ethical obligation of organizations to obtain informed consent from individuals before collecting or sharing their data. IT professionals emphasized that transparency is crucial for building consumer trust and preventing customer loss. They suggested using clear and simple language in privacy policies, providing users with explicit opt-in and opt-out options, and utilizing consent management platforms. This not only aligns with moral principles but also strengthens customer relationships and helps organizations remain competitive in the market. Participants emphasized that obtaining consumer consent is crucial for data privacy. Participant RA-6 mentioned, Once a user or consumer gives his or her consent, it means at least these individuals have some kind of trust in that company.

Participant SD-2 added, It's concerning how our personal information is leveraged for sponsored content and targeted marketing campaigns without our explicit consent. Participant JR-11 further underscored the importance of providing detailed consent options to build trust and ensure transparency and consumer control in data collection. Participant SD-2 disclosed that prioritizing user consent aligns with moral principles and also strengthens customer relationships and

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

boosts market competitiveness. Organizations can build stronger relationships with their customers by providing detailed consent options and creating a more trustworthy digital environment

IX. LIMITATIONS

The researchers faced several inherent limitations in this qualitative study on consumer data privacy and monetization, which impact its generalizability and objectivity. Key challenges included a small sample size selected through convenience sampling, which introduced selection bias and limited the diversity of IT professional perspectives. The qualitative approach itself led to heavy reliance on the researcher's interpretation, raising concerns about subjectivity and interpretation bias.

Furthermore, difficulties in accessing participants due to time constraints, privacy concerns, and invalid contact information, along with the reliance on self-reported data and the impersonal nature of online communication tools, further constrained the study's scope and the ability to ensure equal participation in focus groups. While these limitations restrict the external validity and generalizability of the findings, the researcher was mindful of them and took steps to mitigate their impact, emphasizing that the insights, though specific, still offer valuable contributions to the understanding of consumer data privacy and monetization.

Recommendations for Future Research

The findings of this qualitative descriptive study contribute new knowledge to the understanding of how IT professionals describe cutting-edge strategies to monetize data while upholding consumer data privacy. The subsequent recommendations for future research align with the study's stated significance and contribution to scientific knowledge. Based on the results of this study, the following recommendations are proposed:

1. Given this qualitative descriptive study's IT-centric focus, future research should delve into the perspectives of non-IT professionals (consumers). Future research could investigate consumer attitudes toward data collection and sharing practices and explore potential strategies for enhancing consumer data privacy and sharing in the digital era.
2. Given the exploratory nature of this qualitative descriptive study, future research should conduct comparative analyses of various data monetization strategies. This is crucial in identifying the most effective strategies for monetizing data and addressing pressing consumer privacy concerns. Such research would contribute to developing data monetization models that face the ethical challenge of harmonizing business interests with individual rights to data privacy.
3. This qualitative study revealed a desire for increased consumer control and consent options. Future studies should investigate the barriers hindering consumer control over personal data and assess their impact on data sharing, data quality, and monetization strategies.
4. This qualitative descriptive study was limited to IT professionals aged 25 to 65 involved in data collection, storage, sharing, and protection. A future qualitative study is recommended to focus on younger IT professionals below age 25 who will likely be highly engaged in online activities such as social media and e-commerce. This future research could explore how this demographic approaches online data privacy and identify potential strategies to enhance data privacy measures and increase the participation of young people in platform ecosystem data sharing

Recommendations for Future Practice

The findings from this qualitative descriptive study, in alignment with the literature, revealed organizational leaders' role in supporting and empowering IT professionals to embed data privacy in their application or system design. The findings from this qualitative descriptive study provide practical guidance for ethical data collection and monetization. The following recommendations for organizational action are presented.

1. This qualitative descriptive study's findings affirm the critical need for organizational leaders and IT professionals to adopt practical data collection tools and technologies that minimize consumer data collection while maximizing privacy protections. The results indicate that a move towards data minimization practices can help build consumer trust and motivate them to share quality data, which is crucial for data monetization. Adopting technologies that collect only the necessary consumer data can increase operational efficiency, reduce storage costs, and enhance data protection.
2. Business organizations should implement comprehensive data privacy and monetization frameworks. This framework should incorporate key software development activities and data monetization strategies to protect consumer data privacy and ensure adherence to data privacy regulations. The frameworks should outline data collection and application design guidelines, standards, and processes for handling consumer personal information. In addition, these frameworks should include software developers' training and education to build a data privacy culture within the

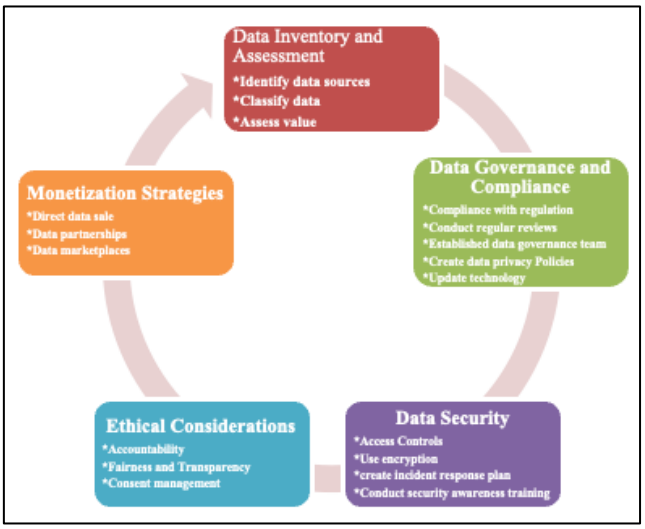
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

organization. This framework can help businesses proactively mitigate data privacy risks, build consumer trust, and avoid costly data breaches. Figure 6 illustrates this framework.

Figure 6: Data Privacy and Data Monetization Framework



3. The evolving landscape of data privacy challenges presented by Artificial Intelligence (AI) and emerging technologies has created a gap in data protection regulations, such as the GDPR and CCPA. The GDPR and CCPA, for instance, need to be modernized to handle the unique data privacy risks associated with AI systems such as large language models (e.g., ChatGPT). Given this, regulators and policymakers must constantly review emerging technology and existing data privacy laws to protect consumers' privacy rights.

The researchers believe that the findings from this qualitative descriptive study and recommendations are applicable to all stakeholders involved in the complex landscape of monetization and consumer data privacy. For instance, software developers can leverage data collection techniques and tools identified in this qualitative descriptive study to design privacy-preserving applications. Again, businesses can implement the recommended data management tools and technologies to protect their enterprise data. These recommendations can help enterprise data protection and instill confidence in data handling practices. Moreover, data privacy regulatory agencies and policymakers can utilize this qualitative descriptive study's recommendations to revamp the current data privacy regulations and the challenges of the rapidly evolving technological landscape.

X. CONCLUSION

This qualitative study explored how U.S IT professionals utilize innovative strategies like data anonymization, consent management, monitoring techniques, and blockchain technology to manage data monetization and consumer privacy concerns. Researchers gathered data through 12 semi-structured interviews and two focus groups (six participants each), analyzing the findings using descriptive statistics and Braun and Clarke's (2006) thematic analysis. An inductive coding approach was chosen to allow for the emergence of new themes, resulting in six key themes that directly addressed the study's sub-questions and were compared to existing research for enriched insights.

REFERENCES

1. Alder, S. (2024). Change healthcare reports ransomware data breach to HHS. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
2. Baecker, J., Engert, M., Pfaff, M., & Krcmar, H. (2020). Business strategies for data monetization: Deriving insights from practice. In Wirtschaftsinformatik (Zentrale Tracks) (pp. 972-987). http://dx.doi.org/10.30844/wi_2020_j3-baecker
3. Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection. Scitech Lawyer, 15(3), 24-29.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. Big Data & Society, 8(1), 20539517211017308. http://dx.doi.org/10.1177/20539517211017308
5. Duan, Y., Ge, Y., & Feng, Y. (2022). Pricing and personal data collection strategies of online platforms in the face of privacy concerns. Electronic Commerce Research, 22(2), 539. https://doi.org/10.1007/s10660-020-09439-8
6. Fefer, R. F., & Archick, K. (2021). EU data protection rules and US implications. Current Politics and Economics of Europe, 32(2/3), 255-261. https://sgp.fas.org/crs/row/IF10896.pdf
7. Han, L. M., Zhao, Y., & Zhao, J. (2020). Blockchain-based differential privacy cost management system. ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. http://dx.doi.org/10.1145/3320269.3405446
8. Harris, R. (2020). Forging a path towards meaningful digital privacy: Data monetization and the CCPA. Loy. LAL Rev., 54, 197. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lla54&div=8&id=&page=
9. Kathoke, K. R., Ravi, p., & Sumant, O. (2022). Data monetization market research, 2030. https://www.alliedmarketresearch.com/data-monetization-market
10. Klaus, T., & Elzweig, B. (2020). The impact of data breaches on corporations and the status of potential regulation and litigation. Law and Financial Markets Review, 14(4), 255-260. http://dx.doi.org/10.1080/17521440.2020.1833432
11. Krafft, M., Kumar, V., Harmeling, C., Singh, S., Zhu, T., Chen, J., Duncan, T., Fortin, W., & Rosa, E. (2021). Insight is power: Understanding the terms of the consumer-firm data exchange. Journal of Retailing, 97(1), 133-149. http://dx.doi.org/10.1016/j.jretai.2020.11.001
12. Line, N. D., Dogru, T., El-Manstrly, D., Buoye, A., Malthouse, E., & Kandampully, J. (2020). Control, use and ownership of big data: A reciprocal view of customer big data value in the hospitality and tourism industry. Tourism Management, 80, 104106. http://dx.doi.org/10.1016/j.tourman.2020.104106
13. Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., Wang, Y., & Weaven, S. K. (2020). Data privacy in retail. Journal of Retailing, 96(4), 474-489. https://doi.org/10.1016/j.jretai.2020.08.003
14. O'Connor, S., Nurwono, R., Siebel, A., & Birrell, E. (2021). (Un) clear and (In) conspicuous: The right to opt-out of sale under CCPA. In Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society (pp. 59-72). http://dx.doi.org/10.1145/3463676.3485598
15. Ofulue, J., & Benyoucef, M. (2024). Data monetization: Insights from a technology-enabled literature review and research agenda. Management Review Quarterly, 74(2), 521-565. https://doi.org/10.1007/s11301-022-00309-1
16. Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: A meta-analytic review. Journal of Retailing, 96(4), 458-473. http://dx.doi.org/10.1016/j.jretai.2020.05.007
17. Parvinen, P. (2020). Advancing data monetization and the creation of data-based business models. Communications of the Association for Information Systems, 47(1), 2. http://dx.doi.org/10.17705/1CAIS.04702
18. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 1-25. http://dx.doi.org/10.1007/s11747-022-00845-y
19. on System Sciences (p. 5676). http://dx.doi.org/10.24251/HICSS.2021.689
20. Ray, J., Menon, S., & Mookerjee, V. (2020). Bargaining over data: When does making the buyer more informed help? Information Systems Research, 31(1), 1-15. http://dx.doi.org/10.1287/isre.2019.0872
21. Rothstein, M. A., & Tovino, S. A. (2019). California takes the lead on data privacy law. Hastings Center Report, 49(5), 4-5. http://dx.doi.org/10.1002/hast.1042
22. Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. International Journal of Information Management, 60, 102331. https://doi.org/10.1016/j.ijinfomgt.2021.102331
23. Wixom, B. H., Piccoli, G., & Rodriguez, J. (2021). Fast-track data monetization with strategic data assets. MIT Sloan Management Review, 62(4), 1-4.
24. Zhang, X., Yue, W. T., Yu, Y., & Zhang, X. (2023). How to monetize data: An economic analysis of data monetization strategies under competition. Decision Support Systems, 114012. https://doi.org/10.1016/j.dss.2023.114012

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com