DIGITAL RIGHTS AND MISUSE OF PERSONAL DATA BY MNCs: A CRITICAL ANALYSIS OF PRIVACY, ACCOUNTABILITY AND REGULATORY FRAMEWORK OF MNCs

S Sri Renganath, SRM School of Law, SRMIST, Chennai

N Sailesh Kumar, SRM School of Law, SRMIST, Chennai

ABSTRACT

In a hyper-connected world such as the one we are living in, in which multinational corporations such as Google, Meta, and Amazon are amassing mountains of personal data, innovation and exploitation have become indistinguishable. In this paper, we will explore in depth just how these tech giants are misusing user data on a daily basis, from sneaky surveillance practices to unauthorized sharing and hyper-targeted advertising, eroding fundamental digital rights and privacy as we know them. From Cambridge Analytica hijacking Facebook user data to influence election outcomes to Zoom faking out security measures and leaking user data everywhere, we will examine the lack of accountability when these tech giants are caught red-handed, from dodging real consequences with fines in change for every dollar of their billions in revenue to hiding behind convoluted legal loopholes.

Zooming out to regulations, the EU's GDPR is the gold standard with strong regulations on consent and data minimization, but MNCs exploit this with jurisdictional shopping. India's DPDP Act is strong on data localization and fiduciary duty, but rollout issues have left users vulnerable to cyber threats. The US A haphazard array of state laws, including CCPA, which only scratches the surface. Through a blend of law, case studies, and economics, this research highlights the gaping holes in regulation, international coordination, and technology, including the absence of mandatory audits of algorithms.

The verdict A radical overhaul is needed, including revenue-based penalties, user-centric tools for control, and international agreements to ensure a level playing field.

In championing a human rights-first approach, this research gives policymakers, activists, and individuals practical answers to address the

excesses of corporations, building a world where privacy is not just a buzzword, but a fundamental right.

Keywords: EU (European Union)[1] GDPR (General Data Protection Regulation)[2] DPDP (Digital Personal Data Protection)[3] MNC (Multi-National Corporation)[4]

LIST OF ABBREVIATIONS

EU - European Union

GDPR - General Data Protection Regulation

BIPA - Biometric Information Privacy Act

DPDP - Digital Personal Data Protection

DPBI - Data Protection Board of India

AI - Artificial Intelligence

MNC - Multinational Corporation

LIST OF STATUTES

Information Technology Act, 2000

IT (Amendment) Act, 2008

Competition Commission of India (CCI)

Biometric Information Privacy Act (BIPA)

Digital Personal Data Protection Act 2023

Justice BN Sri Krishna Committee

[1] The European Union is a union of 27 member states that coordinate policies and laws on trade, rights, and the internal market. It creates binding regulations, such as the GDPR, that apply uniformly across all member states.

[2] The GDPR is the EU's core data-protection law that protects individuals' privacy and controls how personal data is collected and processed. Its main aim is to give people strong rights over their data and ensure lawful, transparent, and secure handling by organisations.

[3] The DPDP Act, 2023 is India's first comprehensive law to protect digital personal data and regulate its processing. It seeks to prevent misuse of data, reduce digital harms, and build a trustworthy environment for citizens and businesses.

[4] An MNC operates across multiple countries and must comply with local laws such as the GDPR and DPDP when handling personal data. Its motive is global expansion, but it must also maintain robust data-governance and respect users' privacy rights.

INTRODUCTION

Digital rights are really about protecting something very simple: our freedom and dignity online.

It's about making sure our personal information stays private, that we're treated fairly, and that we're not quietly manipulated without our knowledge. In India today, many large companies collect huge amounts of data about us what we click, where we go, what we like—often without us fully understanding or truly consenting. This data is then used to build detailed profiles and push targeted ads, sometimes stretching the intent of laws like the 2023 DPDP Act.

At the same time, we've seen serious data breaches exposing millions of people to identity theft, and algorithms that can unfairly affect who gets a loan, a job, or even what opportunities they see. Many apps are also designed to keep us constantly engaged, making it harder to step away and stay in control. All of this points to one thing: we need stronger protections, clearer rules, and genuine, informed consent—so people, not companies, stay in charge of their digital lives.

STATEMENT OF PROBLEMS

The collection and misuse of personal data by multinational corporations has become a major concern. Companies frequently gather excessive information—such as location, browsing behavior, and device data—without meaningful consent, often through long, confusing privacy policies. Users are tracked across platforms, and their data is shared with third parties like advertisers or data brokers without clear awareness. This information is used for targeted advertising and behavioral manipulation, while weak data security measures increase the risk of breaches. Additionally, persuasive app designs encourage excessive engagement and more data sharing, reducing user control. These practices collectively undermine individual privacy, security, and fundamental digital rights, highlighting the urgent need for stronger regulations and effective enforcement mechanisms.

OBJECTIVES

1. To examine how multinational corporations collect, retain, and exploit users' personal data in digital environments.

2. To identify the practices that lead to the misuse of personal data, including tracking, unauthorized sharing, and targeted advertising.

3. To evaluate the effectiveness of existing data protection regulations in safeguarding user privacy and digital rights.

RESEARCH QUESTIONS

1. How do multinational corporations collect, store, and exploit users' personal data, and what practices contribute to its misuse?

2. What are the key regulatory and enforcement gaps that allow multinational corporations to continue misusing personal data despite existing data protection laws?

RESEARCH METHODOLOGY

This research is based on *qualitative doctrinal approach* on Digital rights and misuse of personal data and their weak enforcement against MNCs operating across borders.

This research is completely relayed on Secondary sources and information gathered from different sites.

A qualitative doctrinal research methodology involves a rigorous, subjective analysis of existing legal principles and sources to interpret and synthesize legal doctrine. This method focuses on "black letter" law by examining statutes, case law, and legal literature to identify legal rules, principles, and their underlying theories, rather than empirical or factual data.

REVIEW LITERATURE

Justice BN Sri krishna Committee

"A Free and Fair Digital Economy" was constituted in July 2017, which submitted its report in 2018. The Report had recommended that the right to be forgotten may be adopted based on fivepoint criteria, including: Sensitivity of data, Scale of disclosure or degree of accessibility, Role of DP in public life. Relevance of data to public, Nature of disclosure and activities of data fiduciary. The Committee emphasized on the need for right to be forgotten to be included in the fundamental right to privacy.

India's first comprehensive law for the regulation of the processing of **digital personal data, the Digital Personal Data Protection Act, 2023 (DPDP Act),** came into force on 11th August 2023, after years of judicial directives like the Puttaswamy judgment, which held that privacy is a fundamental right. The law covers digital personal data collected online or digitized offline in India, as well as extraterritorially where the data is targeted at Indian data principals, imposing obligations on data fiduciaries, who decide the purpose and means of processing. Obligations of Data Fiduciaries include ensuring data accuracy, security, notification of breaches to the Data Protection Board of India (DPBI), and erasure of data after purpose (storage limitation, except for government purposes). Data Principals have rights like access, correction, erasure, grievance redressal, and obligations like honest disclosure without impersonation.

The Data Protection Board of India, constituted by the Central Government, will deal with inquiries, impose penalties of ₹250 crore for breaches, and mitigation

COMPETITION COMMISSION OF INDIA Suo Moto 23 In Re:

Updated Terms of Service and Privacy Policy for WhatsApp Users. The choices you have. If you are an existing user, you can choose not to have your WhatsApp account information shared with Facebook to improve your Facebook ads and products experiences. Existing users who accept our updated Terms and Privacy Policy will have an additional 30 days to make this choice by going to Settings > Account. users are required to accept the unilaterally dictated 'take-it-orleave-it' terms by a dominant messaging platform in their entirety, including the data sharing provisions therein, if they wish to avail their service. Such "consent" cannot signify voluntary agreement to all the specific processing or use of personalised data, as provided in the present policy.

Users have not been provided with appropriate granular choice, neither upfront nor in the fine prints, to object to or opt-out of specific data sharing terms

India's Supreme Court has recently issued a scathing rebuke to Meta Platforms and WhatsApp in February 2026 over data sharing practices under their privacy policy, stating that "can't play with the right to privacy of citizens" and may ban their operations if such practices continue. This is in relation to their appeal against a ₹213 crore penalty imposed by the CCI for abuse through data sharing with Meta Platforms' entities. This is also related to DPDP's consent and

fiduciary obligations.

Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)

Patel vs Facebook (2018), BIPA requires a corporation that obtains a person's biometric information to first obtain a "written release" from the customer or the customer's representative. The law also requires a corporation that seeks to obtain biometric information from a customer to first provide "in writing" various information: (1) that the biometric information is being "collected" (2) that the biometric information is being "stored;" (3) the "length of term" that the biometric information will be collected, stored, and used; and (4) the "specific purpose" for the collection, storage, and use of the information.

United States v. Google LLC, No. 1:20-cv-03010

United States v. Google Inc**.** In this case, Google faced scrutiny for its failure to safeguard user information, leading to the leakage of sensitive data. The court held that companies must take reasonable steps to secure user data, and failure to do so could result in harm to the individuals whose information was compromised.

Cambridge Analytica scandal (Facebook fine)

The Cambridge Analytica Scandal: In the Cambridge Analytica scandal, the firm collected information from 87 million Facebook users without their consent through a quiz app, which it then used for political campaign purposes during Trump's campaign in 2016 and Brexit. This resulted in FTC fines against Facebook ($5B) and bankruptcy for Cambridge Analytica.

HISTORICAL BACKGROUND

India's IT laws were not developed overnight but have evolved along with the growth of the internet. In the 1990s, as online transactions and e-commerce activities began to take shape, it was a need of the hour to recognize such activities through laws. In this context, India adopted the United Nations Commission on International Trade Law Model Law on E-Commerce (1996). This led to the framing of the Information Technology Act, 2000, which was enacted and enforced on October 17, 2000. This legislation recognized electronic records and digital signatures and thus facilitated online business and e-governance. It also addressed basic cybercrimes such as hacking and data theft. Nevertheless, it was seen that the growth of

information technology was much faster than the growth of laws. In this context, between 2000 and 2008, issues such as social media misuse, online fraud, and identity theft became common. The government thus introduced the IT (Amendment) Act, 2008. This act added more teeth to laws regarding issues such as identity theft, online cheating, privacy infringement, and cyber terrorism. It also introduced the term "intermediaries," which includes social media platforms.

Later on, a contentious provision (66A) was struck down by the Supreme Court in the case of Shreya Singhal vs. Union of India, which was a major step forward in safeguarding the right to freedom of speech. The guidelines regarding online platforms continued to develop over time— from the guidelines issued in 2011 to the more stringent Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Finally, as data privacy became a major issue, India introduced the Digital Personal Data Protection Act, 2023, which moved the issue of data protection from the IT Act to a specialized area of law.

However, the real start of India's journey towards a proper data protection law was in 2017, when the Supreme Court, in the case of Justice K.S. Puttaswamy vs Union of India, passed a judgment declaring that privacy is a fundamental right. This was a landmark judgment that marked a turning point, as this judgment clearly showed that personal data needs protection.

Subsequently, a Personal Data Protection Bill was drafted by a committee headed by Justice B.N. Srikrishna. This bill was based on user consent, data localization, and the creation of a Data Protection Authority. However, a revised version of this bill was introduced in 2019, which not only increased the government's role but also sought to include non-personal data. This, again, increased the complexity of the law, which not only raised issues of government overreach but also increased the compliance costs for businesses.

However, further review by a Joint Parliamentary Committee in 2021 only added more complexity to this bill. Hence, it was decided by the government to withdraw this bill and come up with a simpler bill. This led to the Digital Personal Data Protection Bill, 2022, which was only focused on digital personal data and tried to minimize compliance issues. Finally, the Digital Personal Data Protection Act, 2023, was passed by India in August 2023. This act introduced a new system of data protection, where the user of the data (Data Principal) has rights over the data, and the organizations handling this data (Data Fiduciaries) must ensure its responsible use. The act also introduced the Data Protection Board of India and penalties up to

₹250 crore. The act is a result of a new era of finding a balance between user privacy and ease of business.

Digital Rights and Misuse of Personal Data by Multi-National Company. A Critically Analysis of Privacy, Accountability and Regulatory Frame Work Of Multi National Company

The growth in the digital economy has significantly impacted how personal data is collected, processed, and monetized. The increasing reliance on digital platforms has brought to the forefront issues such as privacy, consent, and data security. The need to balance innovation, individual freedom, and regulatory checks is being felt in various legal frameworks. In this regard, recent developments in India and globally, through committee reports and landmark judgments, emphasize the need for data protection.The constitution of the Justice B.N. Srikrishna Committee in 2017 marked India's first comprehensive institutional effort to design a structured legal framework for data protection in response to the growing challenges of the digital economy.[5] The Committee's report of 2018 is the basis for developing a rights-based data protection framework in India, emphasizing the significance of privacy, accountability, and control of personal data. This is in addition to having a significant role in developing India's legislation on data protection, including the Digital Personal Data Protection framework. This is in line with the notion that data protection is a fundamental right in a digitalizing society. The Committee has successfully struck a delicate balance between individual rights to privacy and legitimate interests of the State and businesses. One of the Committee's key contributions was its recognition of the Right to be Forgotten as an essential component of the broader Right to Privacy, which had already been declared a fundamental right by the Supreme Court in *Puttaswamy v. Union of India*. The Committee proposed a nuanced framework for implementing this right, based on a five-point criteria: Sensitivity of the personal data ,Scale of disclosure or accessibility, Role of the data principal (individual) in public life ,Relevance of the data to the public AND Nature of disclosure and conduct of the data fiduciary This ensures that the right is not absolute but is balanced against the interests of society and freedom of expression. The Committee was quick to point out that individuals should be in control of their information, especially in terms of how long it is accessible in the cyber world.

[5] The Justice B.N. Sri Krishna Committee , constituted on July 31, 2017, by MeiY, marked India's first comprehensive institutional effort to design a structured legal framework for data protection amid digital economy challenges.

It further highlights the importance of a fair evaluation by a competent body, so that the right to be forgotten is exercised without limiting information in a biased manner.

The issue of meaningful consent in digital markets came under scrutiny in the Competition

Commission of India (CCI) Suo Moto In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users. WhatsApp , a dominant messaging platform, introduced updated terms requiring users to accept extensive data-sharing provisions with its parent company, Facebook. While users were technically given a choice, the structure was effectively a "take-it-or-leave-it" model forcing users to accept all terms to continue using the service. The CCI observed that such consent cannot be considered free or voluntary, especially when, users lack granular control over specific data-sharing aspects, there is no real alternative platform due to market dominance and the terms are imposed unilaterally without negotiation This case is a good example of how competition law and data protection law interact. It shows that dominance in digital markets can undermine user consent. It is a good reminder that privacy is a competition issue, in addition to being a personal right. Exploitative data practices by dominant platforms can be a form of abuse of dominance, even in the absence of price-related harm. This case is a reminder that consent has to be granular and informed, and that consumers should not be expected to agree to complex privacy policies. This case shows that data concentration can be a barrier to market entry, limiting competition and perpetuating dominance. This case is a good reminder that, in digital markets, harm to consumers is no longer limited to economic harm, but includes harm to privacy. The case of *Patel v. Facebook (2018))*[6] in the United States addressed the handling of biometric data, such as facial recognition information. The case was grounded in the Illinois Biometric Information Privacy Act (BIPA), one of the strictest data protection laws globally. The court emphasized that companies must obtain a "written release" before collecting biometric data and must clearly disclose that the data is being collected, that it will be stored, the duration of storage and use and the specific purpose for such collection and use This case also demonstrates the need for informed consent, particularly in cases where the information involved is extremely sensitive, such as in the case of biometric information.

Unlike regular information, information related to biometrics is permanent and uniquely linked to the identity of the person involved, making the exploitation of such information extremely

[6] Patel v. Facebook (2015) addressed the handling of biometric data, such as facial recognition information, under Illinois' Biometric Information Privacy Act (BIPA)

detrimental. The case also demonstrates the need to provide information to the person involved in the processing of their information in a manner that is extremely transparent. The case also demonstrates the need to provide a higher level of protection to information related to biometrics, owing to its permanent nature. The case also demonstrates the legal liability that a corporation may be forced to endure in the event that consent has not been obtained in the manner that it should be. In *United States v. Google Inc*[7]., the issue of data security failures came to the forefront. Google faced scrutiny for failing to adequately protect user information, leading to the exposure of sensitive data. The court held that corporations handling user data have a legal obligation to implement reasonable security measures**.** Failure to do so not only breaches user trust but also exposes individuals to risks such as identity theft, financial loss, and reputational harm. This case reinforces the principle that data protection extends beyond mere consent and encompasses the implementation of proper storage mechanisms, robust cyber security safeguards, and strict accountability for data breaches.

MNCs gather huge amounts of private information (like location, online activity, physical traits, etc.) to do data-targeted ads and build AI programs. Users pay by providing MNCs the "free" services in exchange for sharing their information, but a majority of US users skip over consent forms altogether (56% according to the Pew Research survey).

Concerns about MNC data collection and use by MNCs include:

- Lack of transparency/control: 67% of Americans report they have "little to no" idea how the companies are using their data. 73% of Americans feel they have little to no control over their information once given to a company.

- Profiling/manipulation: Data can create discriminatory targeting (political ads, price discriminatory targeting) and create an addiction to the algorithms, which can be detrimental to mental health, especially in youth, and allows for the spread of false information.

- Global extent: MNCs can track users who have not opted-in to have their information tracked by using cookies and/or third-party trackers. This can allow corporations to

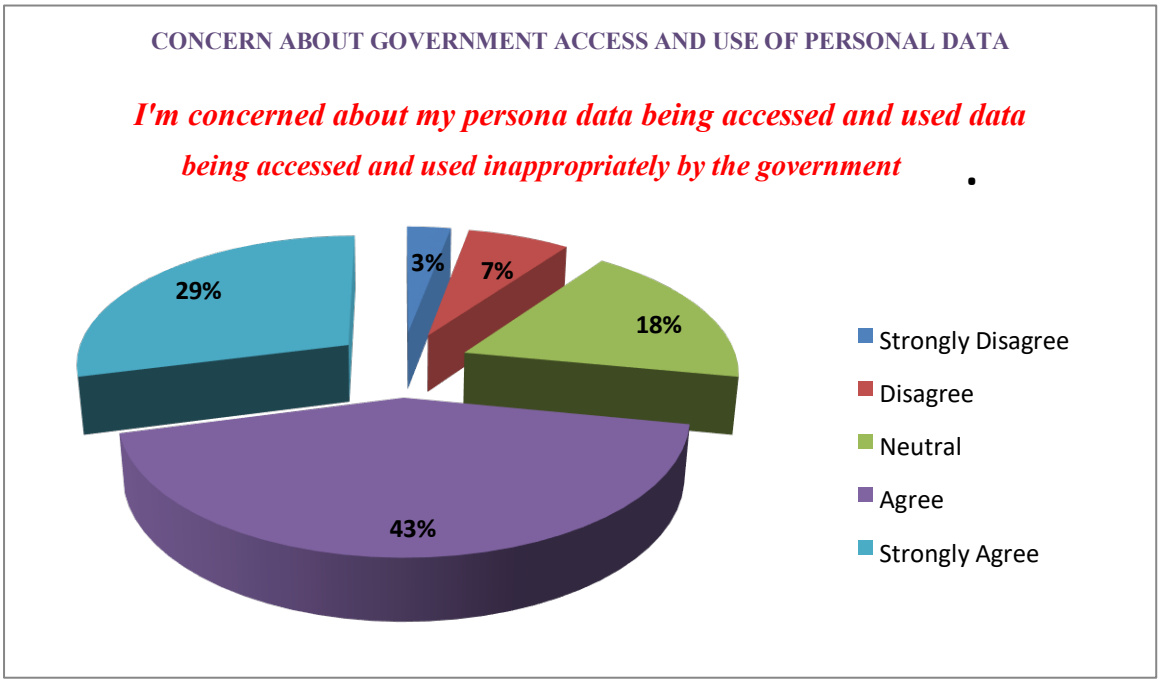
[7] United States v. Google LLC (2020), filed by the DOJ, accused Google of illegally monopolizing the search and ad markets through exclusive default agreements under the Sherman Act

track an individual without their knowledge or consent.

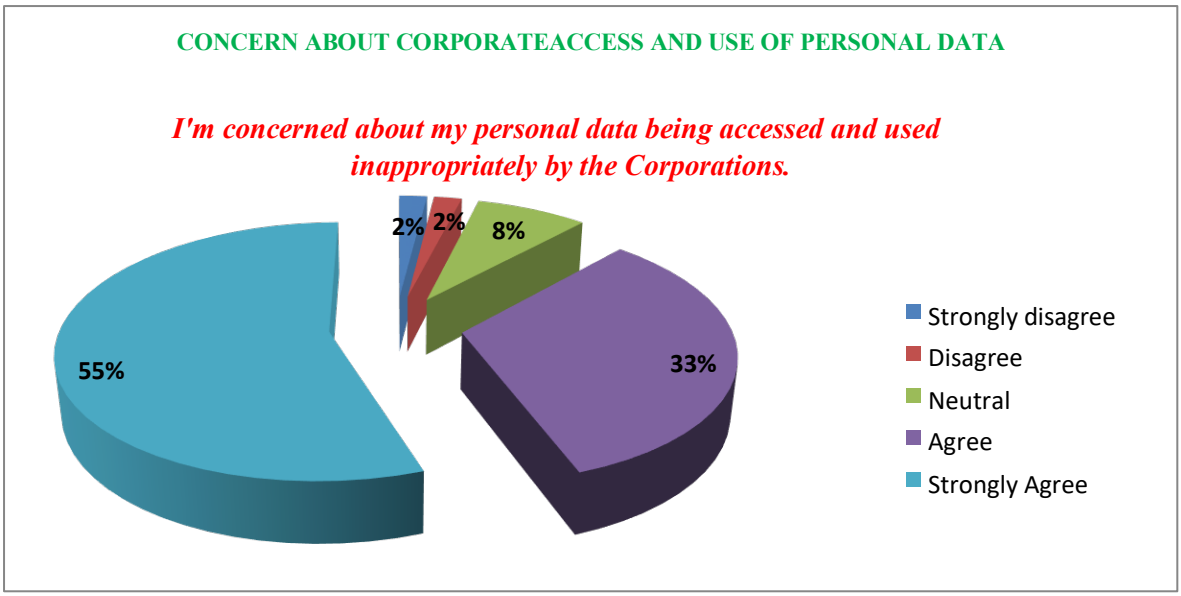
Supporting survey data will be collected through 2025; examples of data collected in 2023 support this information:

- According to Pew Research (2023) 81% of Americans believe the risk to their information being gathered by MNCs outweighs any potential benefits; With regard to government use of personal data, there has an increase from 64% in 2019 to 71% in 2023 with MNC data collection methods adding to the increased lack of trust.

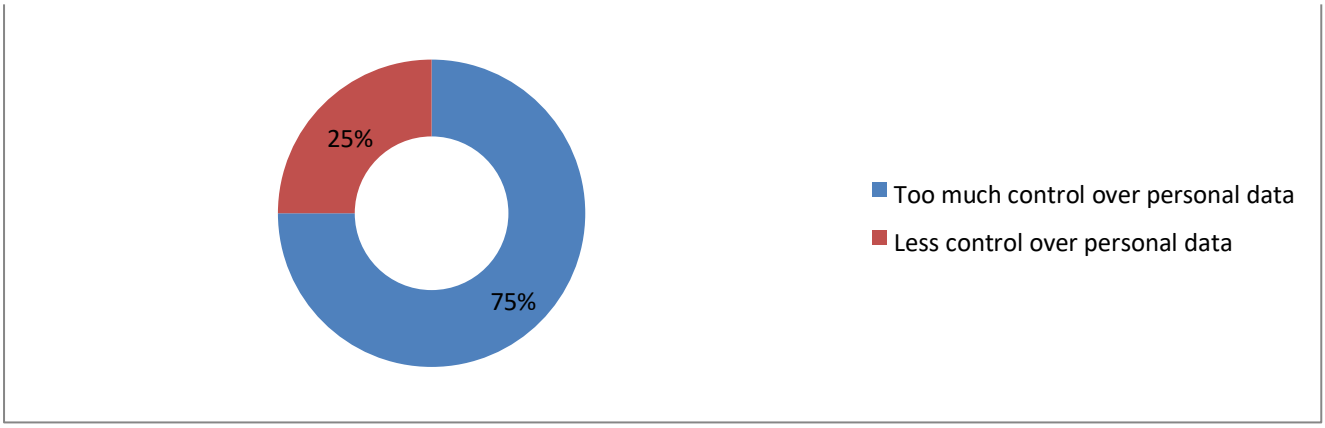
- Malware bytes' Global Survey for 2025[8] shows 56% of respondents agree they are "strongly worried" about corporations 'inappropriately using/accessing personal data,' per graph 1 (compared to the government's 43%). Additionally, 89% of global respondents are worried about AI accessing their data without consent, while 70% have become resigned to the fact that their data will be misused.



[8] Malware bytes' 2025 State of Malware Report highlighted cybercrime's shift to AI-driven autonomous attacks, with agentic AI enabling faster, scalable threats like deep fakes and automated phishing.
Ransomware surged, with 86% using remote encryption and the U.S. hit hardest (48% of attacks), targeting wealthy economies while sparing others geopolitically.



- You Gov Global report on Technology in 2023-2025[9] shows that approximately 75% of adults (especially the older generations) believe that technology companies 'have way too much control over their data.



- Critically, Privacy is not only being breached through hacking but is being structurally undermined with respect to the way the system is designed to operate. Multinational corporations are driven by a profit mindset at the expense of individual rights and have turned the digital world into a form of panopticon for surveillance. This is a violation of core digital rights and significantly impacts those in vulnerable situations.

[9] YouGov's 2023 Technology Trends Report revealed mixed global attitudes toward emerging tech, with 43% believing AI would most improve medical disease diagnosis and 42% favoring travel itinerary planning. Spending on tech declined amid cost pressures, while digital experiences with manufacturers satisfied only 20% of consumers, highlighting privacy and adoption concerns from 2023-2025.

CONCLUSION

The various developments in the above cases collectively reflect the underlying shift in the approach to the concept of personal data in the digital era. Personal data is not merely considered a valuable resource in the economy but rather a significant aspect of the freedom and dignity of individuals, which necessitates the establishment of robust legal frameworks in this regard. In this context, the concept of data retention emerges as a significant aspect in the context of data protection, which necessitates the establishment of clear principles in this regard. In this context, the underlying principle in the context of data retention is the concept of purpose limitation, which necessitates the retention of personal data only for the purpose for which it was originally obtained. In addition to the above, the concept of data minimization emerges as a significant principle in this context, which ensures the retention of only the minimum amount of data required in this context in order to avoid the possibility of data breaches. In this context, it becomes essential for the organization to establish clear retention policies in this context. For this purpose, it is necessary that a system of regular review, such as periodic audits and automatic deletion systems, is incorporated to avoid the accumulation of data that is no longer required. While dealing with sensitive information, including biometric, financial, and health-related data, it is necessary that stricter retention periods are incorporated, given its close relationship with human dignity. Transparency and user control are also very important factors in a good data retention policy. There is a need to educate people about how long their information is being retained, and a right to request deletion or modification of information must be granted. In addition, adherence to relevant legal and regulatory guidelines is a fundamental requirement in order to ensure that organizations are held accountable for their actions, thus preventing possible consequences of non-compliance. Finally, in instances where it is not possible to delete data, anonymization or pseudonymization is a reliable technique that is used in order to ensure that privacy is protected, yet at the same time, data is used in a limited manner.

Thus, a well-regulated data retention policy is of paramount importance in protecting individuals' rights, yet at the same time, it allows for innovation. Conclusion: An effective data retention policy is of paramount importance in order to ensure that the rights of individuals are protected in line with the ever-expanding digital world. This balanced approach, which is based on purpose limitation, data minimization, transparency, and accountability, ensures that the rights of individuals are not compromised in the name of technological and economic

development. At the same time, it helps the organization as well as the State use the data in a proper manner for their legitimate needs. In the end, the importance of data retention practices acts as a link between innovation and data protection, which helps to instill trust in the digital world by respecting the basic principles of autonomy, dignity, and legal fairness.

SUGGESTIONS

Digital rights in relation to multi-national corporations need a stronger and more privacy-centric regime to be in place. The multi-national corporations have to incorporate the principles of privacy by design and data protection by default into their systems, and at the same time, the regulators have to frame regulations around data retention, data sharing, and data transfer, and impose sanctions to ensure that they are followed. Transparency reports and algorithmic audits have to be a requirement to allow public oversight and prevent opaque profiling[10].

At the same time, users' rights have to be enforceable in practice through information that is clear and accessible, consent that is meaningful, and rights to access, correct, delete, and port data. International cooperation and harmonization, like the harmonization of the GDPR and

India's DPDP Act, can also reduce fragmentation in data protection laws and make sure that multi-national corporations behave as accountable data controllers rather than data exploitation machines.

[10] Transparency reports, along with algorithmic audits, hold multi-national corporations accountable for the ways in which they collect, profile, and process personal information. This helps to ensure that the activities of multi-national corporations are aligned with privacy-enhancing best practices, as mandated by the GDPR and the DPDP Act. This helps to prevent the misuse of information, thereby protecting the autonomy, dignity, and right to privacy of individuals from invasive profiling. This helps to ensure that power is matched with proportionate accountability.

REFERENCES

CASE LAWS:

Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017) 10 SCC 1

Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)

United States v. Google LLC, No. 1:20-cv-03010

Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, 133 N.E.3d 723 (Ill. 2019)

Cambridge Analytica scandal (Facebook fine)

BOOKS:

Dr. Rahul Matthan, Data Protection Law in India (2022)

Shyam Divan, Digital Privacy and India's DPDP Act (2023)

Corporate Professionals, Handbook on the Digital Personal Data Protection Act, 2023 book

ARTICLES / JOURNALS:

"From Data Loss to Data Misuse: The New Privacy Threat Model," ECCU Blog (2026). Explores the concept of data misuse, including secondary uses and AI-based profiling, as a more prominent privacy concern than data breaches, particularly for large platforms

UNESCO, "Guidelines for the Governance of Digital Platforms," UNESCO Internet Trust Guidelines (online). Establishes guidelines for transparency, accountability, and human rights-based design for digital platform companies

"Misuse of Personal Data: Case Examples and Consequences," VIDA Blog (2024). Examines personal data misuse consequences for individuals and corporate accountability

Bare-Acts / Official Documents)

Digital Personal Data Protection Act, 2023 (India – official text) https://www.dpdpact2023.com

DPDP Rules, 2025 (Government of India notification, PDF) https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf

EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 – official text https://gdpr-info.eu