Page 1541 - 1551 **DOI:** *https://doij.org/10.10000/IJLMH.112700*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 1

2022

Data Privacy: Finding the Right Balance Between Data Personalisation and Consumer Privacy

MANU MARIYAN ABRAHAM[1]

ABSTRACT

In the new millennium, personal data is a type of virtual currency. Personal data has a high monetary value and continues to rise, and corporations are rushing to capitalize on this trend. Companies that see consumer data as a valuable corporate asset have spent a lot of money on software that makes it easier to obtain it. When personal data becomes a commodity, the question of whether or not legislative restrictions on data exchange are required arises; regardless of their flaws, the two concepts should not be considered mutually exclusive. Data can be collected openly and securely. Making sure to just collect what you need is a start in the right way. Apart from the obvious fear of being chased around the internet for not deciding whether to buy a certain product or not, we are faced with another underlying concern, i.e., the fact that each of our clicks on the internet is stored as digital data and our digital footprint is being analyzed, filtered and owned by the big corporations. Indian Laws are mostly silent regarding data privacy and protection, affirming the age-old saying that legislations never catch up with technology. There have been initiatives to introduce a data protection bill which we hope would be sufficient enough to protect our personal data. With this paper, I would like to touch upon the perils of Data Personalisation and propose, if possible, some remedies to it.

I. INTRODUCTION

I came across the term 'data personalization' in a docudrama called 'The Social Dilemma', which came out in 2020. Then, it was accused of being used as a medium for political microtargeting with respect to elections in different nations. Now, we see the effects of data personalization everywhere we turn. While browsing through the internet, everywhere we see the pictures of that one dress or apparel that we wished to purchase but didn't. It feels like we are being pursued by some unknown force to purchase this certain commodity.

This isn't a new concept; "CRM" (Customer Relationship Marketing) first entered the

[1] Author is a LLM student at Christ (Deemed to be University) India.

 [ISSN 2581-5369]

corporate lexicon in the 1990s, and it was front and centre in the days of Web 1.0 when computers were supposed to be able to do what they still can't: use data to identify customers. Email marketing campaigns were one of the first channels to implement personalized messaging - once, this was limited to simple name recognition; today, the email elite may deliver emails based on an individual's previous activity, such as transactions and searches. The term "personalization" in travel comes from the term "merchandising," which refers to how airlines might increase sales by offering varied options—around 2007, merchandising appeared in global distribution systems' sales and marketing collateral.

Apart from the obvious fear of being chased around the internet for not deciding whether to buy a certain product or not, we are faced with another underlying concern, i.e., the fact that each of our clicks on the internet is stored as digital data and our digital footprint is being analyzed, filtered and owned by the big corporations. To make matters worse, they could sell this information to the highest bidder, as we saw in the case of Cambridge Analytica and AggregateIQ.

Indian Laws are mostly silent regarding data privacy and protection, affirming the age-old saying that legislations never catch up with technology. There have been initiatives to introduce a data protection bill which we hope would be sufficient enough to protect our personal data. With this paper, I would like to touch upon the perils of Data Personalisation and propose, if possible, some remedies to it.

II. PRIVACY IN THE NEW AGE: INFLUENCE OF PERSONALIZATION

In the new millennium, personal data is a type of virtual currency. Personal data has a high monetary value and continues to rise, and corporations are rushing to capitalize on this trend. Companies that see consumer data as a valuable corporate asset have spent a lot of money on software that makes it easier to obtain it. When personal data becomes a commodity, the question of whether or not legislative restrictions on data exchange are required arises. However, legal experts concerned with information privacy have been wary of classifying personal data as a kind of property and have argued for a ban on data trading rather than transferability limits. Other legal professors, on the other hand, have called for the propitiation of personal data but with little regard for privacy concerns.

Many Internet companies acquire a lot of personal data from their customers and use it to target and customize adverts for advertisers. Personalized ad material on such sites may appeal to customers and be better matched with their preferences. Even so, if people perceive the company has breached their privacy, they may find it strange and off-putting. Consumers may

 [ISSN 2581-5369]

"respond" to the ad's appeal as a result of their concerns about privacy. Reactance is a motivational condition in which customers reject coercion by acting in ways that are the polar opposite of what is expected of them.

Internet companies are undecided about whether they should address such issues directly by enforcing stricter privacy rules. Because behavioural research demonstrates that consumer perceptions of control lessen reactance, this might theoretically minimize the potential for customer reactance and boost online advertising performance. Even if the rules are only marginally related to the area where reactance is elicited, this reduction in reactance holds true. Patients with cancer, for example, are more likely to stick to stringent treatment regimens if they feel that they have some control over another element of their medical care. However, addressing consumer privacy concerns while also using consumer data to personalize ads runs the danger of making users less likely to respond to such ads. As a result of this ambiguity, an empirical question about how tightening privacy measures affects advertising performance has arisen.

For the first time, the public is receiving a behind-the-scenes look at Facebook (and, by extension, the whole internet industry) and discovering what appears to be casual attitudes toward personal privacy. The majority of us are only now beginning to realize the near-total aggregation and spread of our internet activities. Many people believe we have been too permissive in enabling firms to gather, store, utilize, and sell our personal information. Simultaneously, both EU-based companies and non-EU-based companies with a global presence face the challenge of implementing measures to address the General Data Protection Regulation (GDPR), a new EU regulation aimed at providing EU citizens with greater transparency and control over their personal data. While the notion appears simple enough, it requires enormous and costly modifications for businesses worldwide.

Facebook's blunders and the looming GDPR are merely foreshadowing of things to come. Even if a formal policy is not in place, businesses must provide consumers with more transparency and the ability to choose their preferred level of privacy and customization. Put another way, they must go to great lengths to develop relationships with their clients and earn their trust.

III. PUBLIC AWARENESS

While the amount of personal data acquired by businesses and organizations have continuously increased, public awareness of the ramifications has not. Many people are aware that data about their tastes, preferences, and whereabouts is used to fuel marketing and content initiatives. Still,

 [ISSN 2581-5369]

only a tiny percentage are concerned about the potential for their privacy to be compromised. Some people are dissatisfied with their lack of control over how much data is collected across the entire internet ecosystem, rather than just the company or platform they signed up for. Some people are worried about being lumped in with groups they believe do not represent them.

To add to the consumer's uneasiness, there appears to be no way to verify exactly what data is being gathered, whether the data is accurate, or how to limit or delete the data if desired. Is the general population waking up from its complacency, which has been fuelled by convenience? Some people wonder if having free access to platforms like Facebook and Google is worth the loss of privacy and the possibility of being micro-targeted to influence purchasing decisions or even political action.

IV. CONCERNS ARE ON THE RISE

The debate over data protection and privacy is still going strong in most parts of the world.

According to Pew Research Center[2], 81 per cent of Americans believe that the risks people suffer as a result of corporate data gathering exceed the benefits.

According to research conducted in Europe[3], 55 per cent of people are concerned about criminals or fraudsters gaining access to their personal information, while around 30 per cent are concerned about advertisers, businesses, and foreign governments gaining access to information without their knowledge. Concerns about security led to legislation such as the General Data Protection Regulation (GDPR), which limits the acquisition and use of personal data.

The public, in general, appears to be more aware of how their data is shared online and how it might be misused, and certain incidents have sparked outrage and hatred toward the companies involved.

V. ARE PEOPLE IN FAVOUR OF PERSONALIZATION?

Personalization is the next step. It's a firm favourite in marketing and customer service since it provides genuine value to both businesses and consumers.

People are aware of this: according to some studies, 80 per cent of customers are more likely to purchase when businesses provide tailored experiences, and 67 per cent believe it is critical

[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, 2019

[3] https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online

 [ISSN 2581-5369]

for brands to automatically change information based on their present context.

All of this, though, comes at a cost. And the cost is data.

Advanced forms, such as hyper-personalization, necessitate the revelation of personal data, such as demographics, preferences, browsing history, purchasing behaviours, and more, to be analyzed and exploited by the corporation using technology (e.g., machine learning). People's data is stored and maintained outside of their control, which appears to be a breach of privacy.

VI. BEST OF BOTH?

So, how does this impact companies? While public opposition to large-scale data collecting is growing, businesses must take the following factors into account:

1. Embrace the spirit of the law

Regardless of how much we enjoy individuality, the law always takes precedence. Before executing any marketing strategy, companies must understand and follow all legal requirements.

This may appear onerous (compliance often may), but it's critical to understand the spirit of privacy regulations. Be customer-centric, in other words. Laws exist to ensure that people's identities are safe with you and that they will receive actual value in exchange for sharing their information.

2. Personal Choice

Enterprises will need to equip products and services with the capacity to choose the level of customization quickly and overtly based on a consumer's willingness to hand over personal information. The demand for a sliding scale of privacy and personalization will be driven by the widespread desire for choice. From marketing efforts to app design, this will have an impact. The following rights must be accommodated by businesses based on GDPR constructs:

- Access – the right to access your data
- Correction – the right to make a correction to any errors that are made
- Erasure – The right to erase data where it is no longer relevant and the right to forbid companies to share data with third parties
- Restriction – the right to restrict the use of your data
- Portability – the right to transfer the said data (processed automatically) to another controller

 [ISSN 2581-5369]

- Object – the right to object to processing
- Informed – the right to be informed of the reasons for processing
- Withdraw – the right to withdraw consent

3. Transparency

Businesses will be forced to raise the curtain — and keep it inflated. The days of blind confidence will be over, and full transparency will be demanded. Organizations will be expected to indicate clearly how they intend to use personal data in simple, easy-to-understand phrases that are free of legal jargon and are clearly marked and highlighted. Companies are already distributing information about their improved data privacy practices to their users. As time goes on, the public will want rules and procedures that are increasingly easier to access, read, and comprehend, as well as a variety of options from which to choose.

4. Enhanced Data Governance

Data governance frameworks in an organization's IT infrastructure will need to be pervasive. "Any information relating to a recognized or identifiable natural person" falls under the definition of personal data. Name, email, address, gender, geography, cultural preferences, an HTTP cookie, and even an IP address are all examples of personal information. "Any operation or combination of operations done on personal data" is what processing of personal data is defined as. It could be as simple as logging an IP address in your web server logs or putting information into an AI engine.

Regardless of citizenship, businesses will need to improve data governance and reconsider how they gather and retain data. They'll have to broaden the data collection that was previously considered sensitive, as well as build and improve data governance wherever consumer data is stored or used. Sales and marketing, contextual data served up via an app, and internal and external data analytics are all examples of this. Companies must also put in the effort to identify, consolidate, and audit the diverse data sources that exist across their whole organization.

5. Align personalization and data privacy efforts

Regardless of their flaws, the two concepts should not be considered mutually exclusive. Data can be collected in an open and secure manner. Making sure to just collect what you need is a start in the right way.

Is it necessary, for example, to know a person's location in order to tailor their experiences?

 [ISSN 2581-5369]

(See below for more information.) According to research[4], "information like name, phone number, and physical address is the data that customers are least okay with marketers obtaining." Purchase histories and goods viewed, for example, are less sensitive than medical or financial data.

Personalization could also learn from customization in this area: personalization is supposed to happen behind the scenes, whereas customization is driven by the user. There may be ways to allow consumers to choose the level of personalization they want (and thus the quantity of data they want to disclose) and tailor their customer journey and experiences, depending on your industry and business.

6. Make better use of aggregate and anonymized data

Granted, personalization entails much more than analyzing anonymous data from all visitors or clients, as well as segmenting the building. This type of data, on the other hand, is considerably easier for customers to swallow and may not raise as many suspicions as a hyper-personalized service. 'Work with what you've got,' as they say.

Amazon, for example, leverages data from a large number of consumers to create the "Frequently Bought Together" section. This allows the business to be relevant to each new customer without alerting them about its data collection methods. You might be able to make better use of aggregate data as well.

7. Privacy by design

Privacy by design is a key concept in privacy legislation; it says that every product or plan you create should address privacy from the start rather than as an afterthought.

This is a great rule to follow since it allows you to strike a balance between personalization and data security because you can provide individualized service while still ensuring that you don't go too far with data collection, storage, and use.

VII. THE INDIAN PERSPECTIVE

The public at large has a right to receive commercial speech. Article 19(1)(a) of the Constitution preserves an individual's right to listen, read, and receive information and ensures freedom of speech and expression.

In the landmark decision of *Tata Press Ltd. vs Mahanagar Telephone Nigam Ltd.*[5] in 1995, the

[4] Chellappa, Ramnath & Sin, Raymond. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management.
[5] JT 1995 (5) SC 647

 [ISSN 2581-5369]

Supreme Court ruled that the rights guaranteed by Article 19(1)(a) of the Indian Constitution could not be denied by granting the government a monopoly. Only the grounds set forth in Article 19(2) of the Constitution could be used to limit it. In this way, the government's ability to intervene was hampered. Advertisers that want to use their freedom of speech and expression to take advantage of a person's right to listen, read, and absorb information can do so with more ease.

With new forms of publication, online commercial advertisements are growing. We now have the means to communicate in real-time. Previously, every home received a newspaper that had 60-70 per cent news, and the remainder was filled with product advertisements, government notices, job openings, and so on.

With the transition to practical means, everyone now has a smartphone in their hand, a desktop at work, and an OTT television at home, all of which keep them connected to the world via service providers such as Facebook, WhatsApp, YouTube, newspapers, websites, e-commerce platforms, and so on, providing them with all of these amenities for free.

VIII. DATA PROTECTION LEGISLATION

The Data Protection Directive was enacted by Europeans in 1995, and the General Data Protection Regulation was passed by Europeans in 2018. (GDPR). There is no distinct data protection law in India at the moment. Explicit provisions for the protection and procedure to follow to ensure the safety and security of sensitive personal information can be found in the rules outlined above.

The impending hazards were highlighted by the 2020 ban on mobile applications on data security. Data has replaced oil as the most valuable commodity on the market. Data is so important in today's world that it may be used to wage war.

Section 43A of the Information Technology Act of 2000, for example, addresses compensation for data security failures.

In 2019, the Lok Sabha debated the Personal Data Protection Bill. It established a Data Protection Authority with the goal of protecting persons' personal data. The bill also holds data fiduciaries responsible and places restrictions on them.

Personal data, for example, can be processed only for particular, clear, and legitimate purposes, with certain goals, collection, and storage restrictions in place. The bill regulates data processing by the government, Indian corporations, and international companies with an actual or potential consumer base in India. Certain types of personal information are labelled as

 [ISSN 2581-5369]

sensitive.

IX. CONCLUSION

Every day, the ordinary consumer is bombarded with hundreds, if not thousands, of marketing messages, the majority of which are ineffective. That is something that no one has time for. Today's customers demand more. They live and work in a digital environment, and they aren't afraid to leave their mark on it through social media, mobile devices, location monitoring, and online participation. They are aware that businesses are monitoring them and expect firms to be aware of their requirements and preferences. They want tailored communications and offers. Businesses may deliver this customization by segmentation, targeting, and engaging customers in relevant one-to-one marketing through the use of big data and more traditional sources of information, along with analytics and data management capabilities. Many customers are also finding that businesses are becoming more adept at tailoring messages.

However, marketers must strike a balance between personalization and consumer privacy. The country's data privacy regulations establish some guidelines for the use of personal data, but these differ by region, complicating the matter even more for worldwide marketers. Furthermore, recent occurrences in the news have increased consumer awareness of data privacy. Consumers are more concerned about who has access to their data and how it is used. Customers' desire to give personal information is driven by their trust in data security, which is unsurprising. In exchange for personal information, most business-to-consumer organizations entice customers with incentives (such as discounts, free shipping, and so on). And it works — at least on the surface. In exchange for a discount on today's purchase, customers frequently submit their names and email addresses. However, when it comes to convincing customers to share more personal information — the kind that helps build a more meaningful relationship – businesses must demonstrate that this information will be kept safe.

Customers must perceive the benefit of sharing their data in the long term. If a customer rarely buys from the company and is concerned about being bombarded with emails in the future, a discount may not be worth it now. Companies must undertake a lot of work to soothe their consumers' concerns about personal information use and security as they use customer data and analytics more extensively.

Customers do not believe organizations are transparent about their personal data practices, and they are unaware of policy revisions. Even more concerning, there is a general lack of trust in the security of personal data. A single news story about a data breach or misuse of personal information can demoralize all customers.

 [ISSN 2581-5369]

As customers continue to adopt technology that allows them to share their life with others, they have two expectations of businesses: to understand me as a person and to respect my privacy.

 [ISSN 2581-5369]

X. REFERENCES

- Elvy, Stacy-Ann. "Paying for Privacy and the Personal Data Economy." Columbia Law Review, vol. 117, no. 6, Columbia Law Review Association, Inc., 2017, pp. 1369–459
- Pavolotsky, John. "Privacy in the Age of Big Data." The Business Lawyer, vol. 69, no. 1, American Bar Association, 2013, pp. 217–25
- O'Connor, Nuala, et al. "Privacy in the Digital Age." Great Decisions, Foreign Policy Association, 2015, pp. 17–28
- Schwartz, Paul M. "Property, Privacy, and Personal Data." Harvard Law Review, vol. 117, no. 7, The Harvard Law Review Association, 2004, pp. 2056–128
- Tucker, Catherine E. "Social Networks, Personalized Advertising, and Privacy Controls." Journal of Marketing Research, vol. 51, no. 5, American Marketing Association, 2014, pp. 546–62
- Fromholz, Julia M. "The European Union Data Privacy Directive." Berkeley Technology Law Journal, vol. 15, no. 1, Temporary Publisher, 2000, pp. 461–84
- Chung Hun Lee, David A. Cranage, Personalization–privacy paradox: The effects of personalization and privacy assurance on customer responses to travel Web sites, Tourism Management, Volume 32, Issue 5, 2011, Pages 987-994, ISSN 0261-5177
- Oppenheim, C. (2012). Data protection and privacy. In The No-nonsense Guide to Legal Issues in Web 2.0 and Cloud Computing (pp. 57-74). Facet.
- Tavani, Herman T. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy." Metaphilosophy, vol. 38, no. 1, Wiley, 2007, pp. 1–22
- Hughes, Kirsty. "A Behavioural Understanding of Privacy and Its Implications for Privacy Law." The Modern Law Review, vol. 75, no. 5, Wiley, 2012, pp. 806–36

*****

 [ISSN 2581-5369]